RUSSELL ROPE
ID 1607 POB 1198
Sacramento, CA 95812
310-663-7655
justice@russellrope.com
In Pro Per

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

RUSSELL ROPE,	Case No.: 25STCV16692
Plaintiff,	
v.	**PLAINTIFF'S RESPONSE TO**
COINBASE, INC. & DOES 1-20,	**DEFENDANT OBJECTIONS TO**
Defendants.	**DISCOVERY**

I. INTRODUCTION

Plaintiff Russell Rope respectfully submits this response to Defendant Coinbase's blanket

objections to Plaintiff's discovery requests and unauthenticated exhibits. Every item Plaintiff

seeks is directly relevant to identifying the unnamed wrongdoers (Does 1-20) and to proving the

ongoing pattern of digital and financial misconduct at issue in this action.

II. GOOD-FAITH EFFORT & PROPORTIONALITY

Plaintiff has acted in good faith throughout. Each request was crafted to obtain specific, necessary facts such as IP logs, transaction records, custody metadata, and communications that can identify the individuals who stole or tampered with Plaintiff's property. No request is harassing or duplicative. Plaintiff is an individual litigant working without pay; Defendant is a hundred-billion-dollar Corporation represented by a full law firm; technically multiple firms and appearances of six attorneys thus far. The burden falls entirely on Defendant only because of its own refusal to resolve the matter when first notified. All of their wounds are self-inflicted results of their refusal to return assets now classified as stolen. This could have been resolved customer support, should have been resolved upon official legal demand, and without excuse for prolonging return of assets beyond the filing of a civil suit.

Every hour Plaintiff must spend litigating is an hour taken from business operations and livelihood; Defendant's counsel is compensated for the same time. The injury to Plaintiff is real and ongoing, whereas Defendant's claimed "burden" is self-inflicted.

Defendant's objections repeatedly claim that Plaintiff's requests are "vague," "ambiguous," or "seek improper legal conclusions." This is inaccurate. Each request was narrowly tailored and easily understood in context. Any alleged ambiguity could have been clarified through meet-and-confer rather than blanket refusal. Plaintiff remains willing to explain the logic and purpose of each request to avoid gamesmanship.

Proportionality and Good-Faith. Every request has a specific purpose: identifying Does 1–20, tracing asset custody, and confirming restoration feasibility. If Coinbase disagreed with any one phrase, the good-faith path was to answer what it could and explain the narrow remainder. Instead, it offered non-specific boilerplate ("vague / ambiguous / overbroad"), which is the very definition of a blanket objection.

III. RELEVANCE TO IDENTIFYING DOES 1-20

All requested materials bear directly on the identities and actions of Does 1-20. Without Coinbase's internal records and data logs, Plaintiff cannot discover who accessed, transferred, or manipulated his digital assets or accounts. Under CCP § 474 and § 2017.010, such discovery is expressly authorized to ascertain unknown defendants. Each objection that refuses basic identifying information undermines the truth-seeking function of this Court and benefits only concealment.

All requested facts—IP logs, transaction metadata, asset custody data, and internal communications—are relevant to identifying who committed the theft, tampering, and fraud. These are not hypothetical inquiries but direct attempts to answer who, what, when, where, how, and why the acts occurred. Defendant's objections ignore that this discovery directly exposes the perpetrators and motive, both central to Plaintiff's claims.

IV. IMPROPER BLANKET OBJECTIONS, BOILDER PLATE CLAIMS & BAD FAITH

Defendant's wholesale refusal to respond on the basis of the stay and generic boilerplate phrases violates California discovery rules (CCP §§ 2030.290, 2031.300, 2033.280; CRC 3.1345).

Blanket objections are improper and presume that every request is burdensome or irrelevant without showing how. The Court should treat Defendant's responses as a failure to respond and order further answers once the stay is lifted.

Privilege and Crime-Fraud Exception. Coinbase's blanket invocation of privilege is improper. Plaintiff's requests seek factual information—identity of actors, transaction records, and account-access data—which are not attorney-client communications or attorney work product. To the extent privilege is claimed, the crime-fraud exception (Evid. Code § 956) applies because the materials appear to have been used to further or conceal ongoing criminal conduct. Sensitive data can be redacted or filed under seal; secrecy is not a defense to transparency in a fraud investigation.

Defendant's strategy mirrors the same procedural obstruction used by prior defendants in Plaintiff's 2017 RICO action: avoid substance, bury the facts in procedure, and deprive Plaintiff of access to justice. Such tactics support a finding of bad faith and further justify lifting or narrowing the stay.

Coinbase's objections are intentionally vague and conclusory—more akin to "throwing darts in the dark" than providing specific factual responses. Their repeated use of "or" and "and/or" without specificity exemplifies improper boilerplate. If Coinbase does not understand a term, it should seek clarification, not use ignorance as an excuse to withhold evidence. Such conduct is not in good faith.

Their invocation of attorney–client and work-product privileges is also overbroad. Factual

information—such as the identity of responsible individuals, technical feasibility of asset

recovery, and internal handling of Web3 wallets—is not privileged. Moreover, any

communication used to further or conceal criminal conduct falls under the crime–fraud exception

(Evid. Code § 956). Sensitive data can be redacted or filed under seal; secrecy is not a defense to

transparency in a fraud investigation.

Coinbase's own conduct has created the burden it now complains of. It could have saved months

of litigation by identifying the responsible individuals, returning the stolen assets, and

negotiating fair compensation. Plaintiff asserts that at least one outside actor is feeding non-

public information to a Coinbase insider. This discovery seeks to expose that connection and

bring those responsible to justice.

Defendant's objections lack foundation and personal knowledge, offer no specific factual

support, and improperly draw legal conclusions. These boilerplate refusals show bad faith and

should be overruled.

V. CONCLUSION

Claims involving fraud, misrepresentation, wrongful deprivation of access, or malicious

interference with property are not subject to private arbitration, and no stay may be used to

conceal or delay investigation into criminal conduct

Plaintiff respectfully requests that the Court:

1. Overrule Coinbase's objections and deem all requests relevant to the identification of

   Does 1-20;

2. Order Coinbase to provide complete responses once the stay is modified or lifted; and

3. Award any appropriate sanctions or relief under CCP § 2023.030 for misuse of the

   discovery process.

Additional point-by-point responses to all of Coinbase's objections are incorporated by reference

and attached as Exhibit A.

Respectfully submitted,

Dated: November 12, 2025

/s/ Russell Rope
Plaintiff In Pro Per

EXHIBIT A

I. PLAINTIFF'S RESPONSE TO DEFENDANT COINBASE'S GENERAL OBJECTIONS TO INITIAL DISCOVERY

II. PLAINTIFF'S RESPONSE TO DEFENDANT COINBASE'S OBJECTIONS TO PLAINTIFF'S FIRST SET OF REQUESTS FOR ADMISSION (1–8)

III. PLAINTIFF'S RESPONSES TO DEFENDANT'S OBJECTIONS TO RFP (1–10)

IV. PLAINTIFF'S RESPONSES TO DEFENDANT'S OBJECTIONS TO ROGS (1–10)

VI. CONCLUSION

November 2025

EXHIBIT A

I. PLAINTIFF'S RESPONSE TO DEFENDANT COINBASE'S GENERAL OBJECTIONS TO INITIAL DISCOVERY

A. GENERAL RESPONSES TO BOILERPLATE

Improper Legal Conclusion.

Discovery Filed Prior to Stay.

All relevant to discovering identities of Does, proving responsibilities, intent, and nothing nearly as vague or ambiguous as an objection saying this or this or this rather than this and this and this. Coinbase's approach is unsupported, conclusory, and legally insufficient as discovery objection. I can explain the logic behind each request and am glad to explain anything the attorneys do not understand.

Privilege – blanket and improper. Coinbase's blanket invocation of privilege is improper. Plaintiff's requests seek factual information—identity of actors, transaction records, and account-access data—which are not attorney-client communications or attorney work product. Moreover, to the extent any privilege is claimed, the crime-fraud exception (Evid. Code § 956) applies because the materials appear to have been used to further or conceal ongoing criminal conduct.

All requests are relevant to discovering identities of Does, proving responsibilities, intent, asset recoverability, public-interest Web3-asset status, and determining who, what, where, when, how, and why these events occurred. Coinbase is using blanket objections with truly vague and

ambiguous claims they hope cover everything without specifying details. Some of these discoveries—with subpoenas in queue—are the exact opposite of their narrative, such as the technical feasibility of asset recovery and Coinbase's handling of Web3 wallets other users surely have not transferred. Their own vagueness about what "cease of service" truly entails is extremely suspect and is being questioned by users publicly.

Plaintiff is only seeking information to expose criminal frauds at the core of this case, which Coinbase is attempting to misdirect the Court from by omitting these claims entirely while focusing on the illusion of their Terms of Service—all of which are negated by criminal conduct. Sensitive data can be kept confidential, sealed, or redacted. Secrecy is not a defense.

The defense is unsupported—allegations of "vague, ambiguous," dart-in-the-dark objections missing the target. "Or or or or or or or" is not definitive; specifics are required. Requests are very specific and those "all" or "any" references are necessary. Defendants must be no less specific than the requests. Whether attorney or judge, if you do not understand a word or term then it is your duty to look it up or simply ask Plaintiff to explain. These are lazy cop-outs. Truly vague and ambiguous, non-specific citations. That is like me saying "I object because of the Constitution."

All requests have purpose. They simply do not want to get caught. A good-faith effort would be doing as much as they can and explaining specifically what they could not do and why. Bad faith is throwing out all of my questions because they do not like one of them. This is not all-or-nothing. There is no way all of these facts or events do not exist or did not take place. Otherwise

we would not be here. All of this lacks foundation and personal knowledge, and is missing

specific factual support, and draws legal conclusions.

Coinbase is creating its own burden by failing to cooperate. They could save a lot of time and

bypass most discovery if they simply admitted who the responsible individuals are. Plaintiff

asserts that at least one person with motive to cut Plaintiff down is feeding at least one high-

ranking Coinbase employee non-public information. That criminal must be brought to justice,

while Coinbase can buy its way out by identifying the racketeer, returning assets, and negotiating

fair compensation.

Coinbase's objections to authentication are unfounded. Digital records such as screenshots, chat

logs, and system messages are authenticated under Evid. Code § 1552 and People v. Goldsmith

(2014) 59 Cal.4th 258, which require only that the proponent show the item is what it purports to

be. Plaintiff maintains original copies, metadata, and recordings and can lodge them with the

Court if required.

II. PLAINTIFF'S RESPONSE TO DEFENDANT COINBASE'S OBJECTIONS TO

PLAINTIFF'S FIRST SET OF REQUESTS FOR ADMISSION (1–8)

A. RFA OBJECTION RESPONSES

- **RFA 1** – Totally unsupported and conclusory, framed as "mandatory." Claims such as

  fraud are exceptions to any arbitration clause and well within the judge's discretion.

  Given the case context, Plaintiff simply asked Coinbase to admit that the lockout was not

caused by personal error as they falsely asserted in their Petition to Compel Arbitration. They are dodging responsibility for misdirecting the Court.

- **RFA 2** – Again conclusory, written as if they already have a ruling granting arbitration. This is essentially the opposite of the previous RFA, asking them to admit that Coinbase locked Plaintiff out—not user error. They must answer the factual question.

- **RFA 3** – Conclusory and evasive. This Request asks Coinbase to admit the obvious technical reality: if you create it, you control it. Refusing to return Plaintiff's assets is not technical infeasibility—it's strong-arm robbery. Coinbase has provided no authenticated technical evidence that recovery is impossible; its own engineer's declaration only hinted that recovery requires collaborative retrieval of a passkey half stored on-device and half server-side. Other technical references indicate the passkey should be recoverable from server-side cache. If Coinbase claims it is not, they must show why recovery was disabled or data destroyed. Otherwise, this is concealment of material technical facts.

- **RFA 4** – All contain the same conclusory "mandatory arbitration" refrain, which is a legal argument, not a discovery response. These RFAs could directly lead to Doe discovery and must be answered.

- **RFA 5** – Fact reflected in docket evidence. After allegedly returning funds to the main Coinbase account (in USD from Plaintiff's bank), Coinbase deactivated use of Plaintiff's

USDC debit card, preventing access to those funds. This fits a documented pattern of financial interference and fraud extending beyond Coinbase, already detailed in Plaintiff's prior RICO filings. These facts require mandatory discovery and amendment of the verified Complaint. If Coinbase cannot admit what is plainly visible, every word they offer deserves caution and doubt.

- **RFA 6** – Already admitted in email correspondence that can be introduced as evidence. Issuing a pretentious refund confirms the facts sought here. Refusal to answer now shows non-compliance and lack of good faith. Plaintiff believes this pattern continues through stalking, psy-ops, and entrapment tactics. Non-answers here reinforce that pattern.

- **RFA 7** – Already proven; shows lack of intent to accept responsibility. Coinbase continues to deny established facts. Their "legal conclusion" objection is meaningless where the RFA addresses conduct, not law.

- **RFA 8** – Seeks discovery of Does 1-20 and possible collusion with prior RICO defendants. All relevant, all factual. Their "argumentative" objection is another generic dodge. RFAs test a party's position on facts—this one does exactly that.

B. RFA CONCLUSION

Every RFA has a defined purpose: to identify the actors, uncover motive, and prove feasibility of restoring Plaintiff's assets. Coinbase's objections are blanket, vague, and conclusory; they hide

facts rather than protect privilege. They show no genuine effort to comply. All objections should be overruled, and Coinbase compelled to provide full, substantive responses within ten (10) days of the stay being lifted.

III. PLAINTIFF'S RESPONSES TO DEFENDANT'S OBJECTIONS TO RFP (1–13)

A. REQUESTS FOR PRODUCTION

- **RFP 1** – It is completely reasonable to request all information relating to Plaintiff's own Coinbase account, including logs, correspondence, and settings. Such data are uniquely within Coinbase's possession and necessary to determine the true cause of the lockout and the reactivation of billing for a cancelled Coinbase One account. These facts establish intent and Doe identities. Plaintiff is not only trying to prove wrongdoing but also to verify the complete truth—if Coinbase acted properly, its own records will demonstrate that. Transparency helps both sides.

- **RFP 2** – This seeks non-privileged communications—e.g., between support staff and internal escalations—to identify who caused or perpetuated the lockout and misstatements. Coinbase may withhold privileged attorney communications, but ordinary operational correspondence must be produced. Providing what can be produced in good faith is expected; withholding everything equates to bad faith.

- **RFP 3** – Requests identification of any third-party entities or developers connected to Coinbase's biometric technology. There is a substantial probability of overlap with

companies and individuals named in Plaintiff's prior RICO claim. Disclosure will clarify whether Coinbase obtained or integrated technology from a source previously tied to similar misconduct.

- **RFP 4** – Seeks records concerning Coinbase's refusal to use alternative login or biometric-override options. Such materials are central to truth-finding and to Plaintiff's claim that Coinbase could have reversed the lockout, particularly after the cease-and-desist letter and Judge Chalfant's directive to explore resolution.

- **RFP 5** – Requests the complete digital paper trail of the Coinbase One refund and related charges. This is a small amount for Coinbase but a substantial loss for Plaintiff, who is in forma pauperis. The pattern mirrors prior financial interference described in the 2017 RICO complaint and shows continuing deprivation of funds. This discovery is mandatory to trace the decision-makers and to evaluate criminal intent.

- **RFP 6** – Seeks documentation confirming or corroborating financial transactions, including bank statements reflecting the disputed transfers. Coinbase is best positioned to identify which responsive records exist. Because Defendant has been unwilling to cooperate, Plaintiff must obtain all potentially relevant data to isolate key evidence for the Court.

- **RFP 7** – Focused on discovering the identities of those responsible for the misconduct. More data yields more certainty. Coinbase created this burden through non-cooperation; it can end it by identifying the responsible individuals, returning assets, and negotiating a fair resolution.

- **RFP 8** – Directly seeks the identity of the individual(s) who deprived Plaintiff of his money. The objection that this is "burdensome" or "harassing" is baseless. It is fundamental to the case.

- **RFP 9** – Requests documentation of any communications between Coinbase and law-enforcement or regulatory agencies regarding Plaintiff. If Coinbase received no inquiries, it can simply state so. If it made or received reports, those communications are relevant to both truth and accountability.

- **RFP 10** – Seeks the identities and reasoning of the individuals who ignored or denied Plaintiff's recovery requests. As a developer, Plaintiff maintains Coinbase could have restored access through passkey retrieval or biometric override. Records concerning those refusals go to capability, intent, and fraud.

- **RFP 11** – Requests communications referencing Plaintiff or his businesses by name (e.g., "Classy Savage"). Such evidence may reveal brand-related misconduct or third-party attempts to appropriate Plaintiff's trademarks. Production is limited and reasonable.

- **RFP 12** – Seeks documentation of the exact version of the Coinbase Terms of Service in effect when Plaintiff created his account and any subsequent modifications. Coinbase has not shown that biometric verification or arbitration provisions existed at that time. Without contemporaneous proof, there is no evidence Plaintiff ever agreed to such terms.

- **RFP 13** – Seeks identification of any non-attorneys with whom Coinbase has discussed Plaintiff or his accounts. Any unauthorized sharing of personal information would corroborate allegations of collusion and data misuse. Coinbase should either identify such communications or affirm none exist.

IV. PLAINTIFF'S RESPONSES TO DEFENDANT'S OBJECTIONS TO PMK TOPICS

Defendant's responses to the PMK topics improperly repeat the same meritless legal conclusion—that these matters are "subject to mandatory arbitration." This ignores the reality that claims involving fraud, malice, theft, digital interference, and patterns of criminal conduct are not arbitrable and cannot be privatized to conceal wrongdoing. These PMK topics seek factual information necessary to identify Does 1–20 and determine who inside or outside Coinbase triggered, executed, or concealed the acts in question. Each topic remains essential.

A. PMK TOPICS OBJECTION RESPONSES

- **PMK TOPIC 1 – Coinbase's decision-making and processes regarding Plaintiff's account lockout.**

Directly relevant to identifying the individuals who authorized, executed, or concealed

the lockout. This should only require a short list of account-specific entries. Coinbase is

obligated to know who handles escalated account actions; refusal strongly suggests

concealment.

- **PMK TOPIC 2 – All audit logs and system records documenting Plaintiff's access and restrictions.**

  Limited, specific, and highly probative. These logs will show when, how, and by whom

  access was cut off. If untainted, they may reveal intentional targeting.

- **PMK TOPIC 3 – Coinbase's ability to override lockouts and restore access.**

  Coinbase has never stated, with technical specificity, that restoration was impossible.

  This topic goes to the heart of false statements, misdirection, constructive fraud, and

  potential ADA violations. As a professional developer, Plaintiff has strong technical

  reasons to believe recovery was feasible. Coinbase must present real answers—not

  attorney conjecture.

- **PMK TOPIC 4 – Policies and contracts relating to biometric vendors.**

  There is a strong likelihood of overlap between Coinbase's biometric systems and entities

  named in Plaintiff's prior RICO claim. This topic is central to understanding whether

  shared vendors, employees, or contractors facilitated the misconduct.

- **PMK TOPIC 5 – Coinbase One cancellation/reactivation processes.**

Plaintiff did not reactivate Coinbase One. Someone with administrative access did. This topic is necessary to determine whether an internal actor, outside actor, or Doe collaborator accessed or modified Plaintiff's data. This goes directly to identity and intent.

- **PMK TOPIC 6 – Coinbase's handling of refunds, including USDC refunds.**
Coinbase refunded money to an account Plaintiff could not access and then deactivated his USDC debit card. These acts cannot be brushed aside as "technical." They indicate targeted deprivation. This topic seeks the digital paper trail.

- **PMK TOPIC 7 – Communications with law enforcement regarding Plaintiff.**
It is important to determine whether: law enforcement contacted Coinbase, Coinbase contacted law enforcement, Coinbase made any false, inaccurate, or malicious reports, or Coinbase concealed complaints. Any one of these affects Doe identification and public-interest aspects of the case.

- **PMK TOPIC 8 – Communications regarding Plaintiff's cease-and-desist.**
This seeks to identify the individuals whose decisions escalated this into litigation instead of resolving it when first notified. Their reasoning, motives, and internal communications are directly relevant.

- **PMK TOPIC 9 – Handling of Plaintiff's NFTs and Web3 wallets after "discontinued support."**

Coinbase's handling (or mishandling) of these assets suggests a possible scheme to

deprive Plaintiff of valuable digital property. This is a public-interest issue, as many users

likely lost access under similar circumstances. This topic is essential.

- **PMK TOPIC 10 – Communications with Does or outside actors regarding Plaintiff.**
  Information is being fed to Coinbase from a malicious third party. This topic seeks to
  expose that coordination. Such communications are not privileged and cannot be shielded
  by boilerplate objections.

B. CLOSING NOTE ON PMKS

Coinbase repeatedly claims topics are "burdensome." They are not. Coinbase can immediately

reduce any burden by telling the truth, identifying the individuals involved, returning Plaintiff's

assets, and negotiating in good faith. Their refusal is what creates burden. Furthermore,

arguments involving attorney-client privilege or trade secrets are overbroad; sensitive materials

can be sealed or redacted. None of those concerns excuse a total refusal to participate.

IV. PLAINTIFF'S RESPONSES TO DEFENDANT'S OBJECTIONS TO ROGS (1–10)

All of Defendant's general objections are overbroad, unsupported, and largely boilerplate. These

Interrogatories seek basic factual information necessary to identify Doe defendants, establish

responsibility, verify access paths, and determine the motive and method behind Plaintiff's

lockout and financial deprivation.

A. INTERROGATORY OBJECTION RESPONSES (1-10)

- **INTERROGATORY 1 –** Identifies all Coinbase personnel who handled or reviewed Plaintiff's account issues. This list is essential to identify Does 1–20 and supports follow-up discovery. Coinbase knows exactly who these people are. Support chat usernames should be included.

- **INTERROGATORY 2 –** Same reasoning as above. This interrogatory helps establish responsibility and clarify the timeline of interference.

- **INTERROGATORY 3 –** Plaintiff has a right to know who his personal information has been shared with. This goes to damages, privacy violations, collusion, and potential crime-fraud activity.

- **INTERROGATORY 4 –** Directly tied to security and identity protection. Coinbase had opportunities to prevent escalation and failed to do so. Identification of the individuals involved is necessary.

- **INTERROGATORY 5 –** Seeks evidence Plaintiff was intentionally targeted and by whom. This includes discovering the identity of Does who performed name hacks, created false narratives, or refused compliance for malicious reasons.

- **INTERROGATORY 6 –** Attempts to identify individuals who acted with malice or collaborated to perpetuate harm. Coinbase must answer.

- **INTERROGATORY 7 –** Identifies any individuals who made false, retaliatory, or misleading reports about Plaintiff, whether internal or external. This helps establish motive and connects to Doe identification.

- **INTERROGATORY 8 –** Interrogatory intended to reveal parties involved in deliberate harassment—particularly "name hacks" and behavior designed to burden or intimidate Plaintiff. These patterns are documented.

- **INTERROGATORY 9 –** Seeks additional actors who may have contributed to the scheme to deprive Plaintiff of access, assets, or financial stability.

- **INTERROGATORY 10 –** Same as Interrogatory 8, focusing on pattern evidence necessary to demonstrate ongoing harassment, obstruction, and potentially criminal coordination.

VI. CONCLUSION

Under California law, Coinbase cannot evade responsibility by refusing to identify the individuals responsible. A corporation is charged with the knowledge and actions of its employees (People v. Toomey, 157 Cal.App.3d 1), and corporate officers may be held liable for

failing to detect or correct misconduct occurring under their authority (U.S. v. Park, 421 U.S. 658). If Coinbase maintains that it "cannot identify" those responsible, then responsibility necessarily rises to executive level, and this Court may impose appropriate remedies under CCP § 187 and § 2023.010.