IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

JACOB KEVYN REPKO, individually and on behalf of all others similarly situated,	**Case No.: 1:25-cv-01319**
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	
KROLL RESTRUCTURING ADMINISTRATION LLC (f/k/a Prime Clerk LLC),	**JURY TRIAL DEMANDED**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Jacob Kevyn Repko ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Kroll Restructuring Administration LLC (f/k/a Prime Clerk LLC) ("Kroll" or "Defendant"). Based upon personal knowledge as well as information and belief, Plaintiff specifically alleges as follows:

NATURE OF ACTION

1. This is a data-breach and negligent-administration class action arising from Kroll's August 19, 2023 security incident and its subsequent failure to administer creditor-facing processes and notices with reasonable care in three large crypto bankruptcies—FTX, BlockFi, and Genesis.

2. Kroll's breach exposed (among other fields) names, addresses, email addresses, phone numbers, claim identifiers/amounts, and copies of proof-of-claim forms—precisely the metadata criminals exploit to target crypto victims with phishing and "wrench" attacks.

3. After the breach, Kroll persisted in email-only critical notices (including FTX's 130th Omnibus Objection, claim verification, and tax form deadlines), despite (a) widespread phishing impersonations that trained many creditors to avoid opening "Kroll" emails and (b) Kroll's

demonstrated ability to send first-class USPS letters when it chose to—e.g., in Genesis, where Kroll mailed breach notices via First Class Mail.

4. Federal bankruptcy courts had sealed creditor PII precisely to prevent crypto-targeting crimes—citing the real-world harms seen in the Celsius bankruptcy (phishing and "wrench" attacks). The Genesis docket memorializes these concerns in orders sealing customer information.

5. Plaintiff Jacob Kevyn Repko (Dripping Springs, Texas) filed an FTX customer claim, then received Kroll's August 24, 2023 breach notice. His PII and claim data were among the data compromised.

6. In the months that followed, the FTX Customer Claims Portal (the "FTX Portal") repeatedly malfunctioned: Plaintiff's KYC showed "Verified," then flipped back to "On Hold/Unverified," blocking him from uploading IRS form (W-9) required to receive distributions, despite dozens of support emails.

7. Because the FTX Portal gates tax-form upload behind "KYC Verified," Plaintiff cannot complete the final prerequisites; under the confirmed plan and trust communications, claims may be expunged or distributions forfeited if tax forms are not timely uploaded.

8. Plaintiff also suffered direct phishing loss following the breach: he transferred 1.9 ETH from an exchange account into his hot wallet at 12:43 PM on July 3, 2025 and it was diverted through an automated transaction bot commonly used to intercept pending transfers to a wallet not controlled by Plaintiff, consistent with Kroll's own warning that attackers would use the leaked data to phish crypto accounts.

PARTIES

9. Plaintiff Jacob Repko is a natural person domiciled in Hays County, Texas. He is an FTX customer-creditor with a scheduled claim of $87,487.93.

10. Defendant Kroll Restructuring Administration LLC is a Delaware LLC with significant operations nationwide, including offices in Texas.

11. Upon information and belief, Plaintiff also sues Does 1-5, presently unidentified non-Kroll entities that participated, if at all, in claimant-facing verification or tax-form intake (including third-party KYC vendors). To the extent any non-Kroll entity controlled KYC status flags or W-9/W-8 gating within the FTX Portal, Plaintiff pleads those allegations in the alternative and will amend and substitute the true names when identified. If Kroll designates any responsible third party, Plaintiff will timely join such party under Texas proportionate-responsibility rules.

JURISDICTION AND VENUE

12. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d) (CAFA): the proposed classes exceed 100 members; aggregate controversy exceeds $5,000,000; minimal diversity exists (Texas plaintiff vs. Delaware/New York defendant with nationwide/international class members).

13. This Court has personal jurisdiction over Kroll because Kroll maintains offices in Austin, Dallas, and Houston, purposefully directs administration/noticing work and claimant communications to Texas, and committed acts causing injury to a Texas resident in this District. Plaintiff's claims arise out of or relate to that forum conduct, and exercising jurisdiction comports with due process.

14. Venue is proper under 28 U.S.C. § 1391(b) because a substantial part of the events and harms occurred in this District: Plaintiff resides here, received Kroll's notices here, used the FTX Customer Claims Portal (claims.ftx.com) and then Kroll's Electronic Proof of Claim ("EPOC") here, and suffered phishing loss here.

15. At this time, Plaintiff does not assert claims against the Debtors, or any plan-released party, and does not seek relief requiring interpretation, modification, or enforcement of the Plan or

Confirmation Order. These are independent tort/contract claims against non-debtor Kroll. This action is not a core proceeding; Plaintiff demands a jury and does not consent to bankruptcy adjudication.

DEFINITIONS

16. "FTX Customer Claims Portal" or "FTX Portal" means the portal at claims.ftx.com operated for the Debtors/FTX Recovery Trust (with vendors) to handle KYC/AML and account review. "Kroll Site" means Kroll's website, including the EPOC interface on restructuring.ra.kroll.com, which received bankruptcy Form 410 submissions and maintained the public claims register. Where control is unclear, Plaintiff pleads in the alternative against Doe Defendants to be substituted when identified.

FACTUAL ALLEGATIONS

A. Kroll's Breach Spanned FTX, Genesis, and BlockFi

17. On or about August 19, 2023, an attacker SIM-swapped a Kroll employee's phone, accessing Kroll's cloud files with claimant data for each bankruptcy estate. Independent threat-intelligence confirms the compromised fields were later monetized and operationalized by fraud actors targeting FTX claimants and secondary-market transactions.

18. Kroll's Genesis filing admits impacted data included names, phone numbers, addresses, claim numbers/amounts, wallet/coin balances, and copies of proofs of claim.

19. BlockFi's notice further details that date of birth, mailing address, and driver's license numbers were involved and recounts Kroll's delayed identification of a large tranche of "Unstructured Files."

B. Courts Sealed Creditor PII Because Crypto Creditors Face Unique Attack Vectors

20. In Genesis, the court entered sealing orders protecting creditor names/contact info, referencing the Celsius experience where phishing and wrench attacks followed public disclosures.

C. Kroll Knew Email Was Unsafe But Failed To Use Postal Mail For Critical Notices

21. On information and belief, Kroll publicly warned Genesis creditors about phishing and sent First-Class Mail breach notices to ensure delivery.

22. Yet in FTX, for equally (or more) consequential notices—including the 130th Omnibus Objection deadlines (e.g., start KYC by March 1, 2025; complete by June 1, 2025) and the tax-form deadline—Kroll relied primarily on email just months after its own phishing-triggering breach, knowing many recipients would not open "Kroll" emails for fear of scams or would find them in spam/junk. Public threat-intel shows phishing-led account takeovers where perpetrators changed claimant emails to fresh ProtonMail addresses and rapidly passed 2FA challenges—precisely the attack Kroll's email-only approach left unmitigated.

23. The FTX Portal gates W-9/W-8BEN upload behind KYC verification. When the portal erroneously flips a user back to "On Hold/Unverified," the tax-form step becomes impossible—risking claim expungement or forfeited distributions under plan processes communicated to creditors. In an environment where claimants are trained to avoid 'Kroll' emails due to active impersonation, a gated, online-only tax-form step without a First-Class Mail fallback was not reasonably calculated to apprise or enable completion.

24. The FTX confirmation order expressly provides that Kroll is not released or exculpated for "Security Incident" claims and that customer damages recoverable in another proceeding are not capped by plan distributions. Plaintiff respectfully requests judicial notice of that confirmation-order excerpt under Fed. R. Evid. 201.

25. In addition to being employed by the bankruptcy court under §156(c) noticing, Kroll was retained as Administrative Advisor to perform bankruptcy administration services under its engagement papers and the Court's retention order. These creditor-facing duties (solicitation/balloting/tabulation and handling claimant communications) support the administration obligations alleged herein.

D. Plaintiff's Experience

26. Plaintiff filed his customer claim using the FTX Portal and, when prompted, lodging the bankruptcy Form 410 through Kroll's EPOC.

27. He received Kroll's breach notice confirming exposure of his name, address, email, and account balance and warning of phishing aimed at crypto assets.

28. After struggling with portal lockouts and delays, Plaintiff's KYC was verified on or around November 3, 2023, yet the portal later reverted to "On Hold," blocking IRS-form upload; countless emails to Kroll went unresolved.

29. Post-breach, Plaintiff was phished: 1.9 ETH was drained minutes after reaching his hot wallet (12:43 PM arrival; 12:49 PM outbound to attacker address).

30. Plaintiff holds a scheduled FTX claim of $87,487.93 and now faces loss of some or all distribution value because he cannot satisfy plan prerequisites due to portal malfunctions and notice failures.

31. Plaintiff suffered concrete injuries including: (a) actual misuse—theft of 1.9 ETH within minutes of arrival to his wallet on July 3, 2025; (b) time-value and distribution harms from blocked verification/tax-form submission; (c) out-of-pocket mitigation costs; (d) loss of privacy/control of PII; and (e) substantial risk of future misuse given the crypto-targeting patterns documented herein.

E. Systematic Misuse of Leaked Claimant Data

32. Foreseeability is no abstraction: investigators traced $5.6 million in fraud exploiting FTX claims data, including dark-web sales of claimant datasets and email-change/2FA-bypass patterns—exactly the harms courts sought to prevent by sealing crypto-creditor PII. Kroll's contrary messaging that no sensitive PII was at risk misled consumers about the need to treat every "Kroll" email as suspect and to demand postal mail backup.

33. Independent threat-intelligence corroborates that FTX claimant data has been actively weaponized against creditors and counterparties. In July-November 2024, investigators documented at least $5.6 million in fraud tied to FTX claims trading, where an actor (or group) impersonated claim holders using AI-altered selfies, fresh ProtonMail accounts, and falsified identification.

34. The actor's tradecraft included: (a) recently created ProtonMail addresses substituted for the claimant's original email; (b) rapid entry of 2FA codes, suggesting account takeover; and (c) laundering through Gate.io, CoinEx, and Binance deposit addresses. These patterns are consistent with phishing-led credential compromise following the Kroll incident.

35. The same research shows FTX claims data advertised on dark-web forums, including names, phones, emails, wallet/transaction details, and other claim-linked data—the exact fields Kroll acknowledged were compromised (names, emails, phone numbers, mailing addresses, account identifiers and balances, and in some cases dates of birth).

36. Investigators also observed email changes to post-shutdown ProtonMail accounts for claims originally opened with different emails, indicating takeover and impersonation of claimant accounts.

37. The report documents blockchain paths from impersonator wallets to CoinEx deposit addresses and identifies an intermediary wallet associated with automated transaction activity; it notes interactions with U.S. exchanges (Coinbase and Kraken) that can be subpoenaed for KYC. This evidences a cohesive, repeatable fraud pattern exploiting claimant PII and workflow weaknesses.

38. The report further notes an "Orbeon Forms – Page Not Found" error surfaced during a due-diligence FTX Portal walkthrough—consistent with a brittle claimant workflow and error states that bad actors can mimic, amplifying confusion in a high-phishing environment.

F. Post-Breach Misrepresentations and Omissions

39. Kroll publicly and in claimant communications downplayed the scope of the breach—stating early on that no sensitive PII had been compromised. In other estates it administered (e.g., BlockFi), Kroll later disclosed that dates of birth were contained in "unstructured data," contradicting its initial statements. Kroll likewise told FTX claimants they could continue interacting with email-based workflows and did not warn that bad actors were impersonating Kroll and changing claimant email addresses to newly created ProtonMail accounts to defeat 2FA—patterns confirmed by independent threat intelligence. These statements and omissions were material, consumer-oriented, and misleading, and they induced reasonable claimants to underestimate risk, continue using email-only channels, and delay stronger remediation, contributing to phishing loss, time-value damages, and missed deadlines resulting in expunged claims.

CLASS ALLEGATIONS

40. Global Crypto-Creditor Class: All persons worldwide whose PII or claim data provided to Kroll for the FTX, BlockFi, or Genesis bankruptcy cases was accessed, exfiltrated, or reasonably at risk in the August 2023 Kroll incident. Class membership is ascertainable from Kroll's notice lists, EPOC records, and the estates' claims registers identifying individuals whose data Kroll admits was accessed or reasonably at risk in the incident.

41. Estate Subclasses: (a) FTX Subclass; (b) BlockFi Subclass; and (c) Genesis Subclass. Plaintiff will add named representatives for the BlockFi and Genesis subclasses at or before class-certification.

42. Injury Subclasses (across estates): (i) Phishing/crypto-loss subclass; (ii) Portal/verification/tax-form subclass (expungement loss, time-value loss, and administrative harm); (iii) Standard data-breach injury subclass (privacy invasion, mitigation costs).

43. Numerosity, commonality, typicality, and adequacy are satisfied: common questions include whether Kroll owed and breached duties of data security, notice adequacy, and claims-

process administration; whether email-only noticing was reasonable post-breach; and whether injunctive relief is warranted.

CHOICE OF LAW

44. Conduct-regulating standards are governed by New York law (Kroll is headquartered and acted from NY), or alternatively Texas law for Texas residents and harms. The claims rise and fall on duties/acts common to all class members. Issues of arbitrability are governed by the FAA; New York public policy bars contractual exculpation of gross negligence.

CAUSES OF ACTION

COUNT I

Negligence (New York law; alternatively Texas law)

45. Kroll owed Plaintiff and the Classes (FTX, BlockFi, and Genesis) a duty to exercise reasonable care in collecting, storing, transmitting, and administering claimant PII and claim data; to design, operate, and support a functional verification/tax-form workflow; and—especially after the August 19, 2023 incident—to give notices reasonably calculated, under all the circumstances, to apprise claimants of rights-affecting deadlines and steps and to mitigate foreseeable phishing and deliverability risks.

46. Those duties arose from (a) Kroll's roles as the court-appointed noticing/claims agent and Administrative Advisor; (b) court orders sealing crypto-creditor PII because of known phishing and physical security risks; (c) Kroll's own knowledge and warnings that exposed claimant emails would be targeted for phishing; and (d) Kroll's control over claimant communications and EPOC intake; to the extent a non-Kroll entity controlled KYC status flags and tax-form gating inside the FTX Portal, Plaintiff pleads those allegations in the alternative against Doe Defendants to be substituted when identified. These duties are independent of any contract and recognized under New York and Texas law where a party's conduct creates or heightens a foreseeable risk of identity/asset

theft to a known, finite class (sealed-PII crypto claimants), and where post-breach notice and process choices are governed by due-process principles (e.g., *Mullane; Jones v. Flowers*) and the bankruptcy court's privacy/notice orders.

47. Kroll breached its duties by, inter alia: (i) permitting the SIM-swap-enabled compromise of cloud repositories holding claimant data; (ii) failing to promptly and completely identify all impacted stores of data; (iii) persisting—post-breach—in email-only notice for rights-affecting communications even though many claimants could not distinguish legitimate Kroll emails from phishing and even though Kroll had the ability and precedent to send First-Class Mail; (iv) allowing a distribution workflow in which W-9/W-8BEN upload was blocked unless KYC showed "Verified" in the FTX Portal, while failing to provide a manual/alternative submission path via Kroll's EPOC or by mail/email; (v) failing to provide any manual/alternative submission path or mailed confirmations for status changes; (vi) providing circular, delayed, or ineffective support that prolonged and compounded the harm; (vii) failing, post-breach, to implement change-control hardening (mailed code to the old address for any email/phone change; forced cooling-off periods; manual review of changes to ProtonMail accounts created after November 2022) despite evidence of email-takeover patterns against claimants; and (viii) failing to deploy dark-web monitoring and look-alike takedowns keyed to FTX/Kroll claim keywords after offers of claimant datasets were observed online.

48. The risks Kroll created and failed to mitigate were foreseeable: federal courts in crypto cases had sealed customer PII to prevent phishing and "wrench" attacks; federal law-enforcement and security guidance warn digital asset holders to keep identifying information private; and Kroll itself told claimants that attackers would send convincing emails to take over accounts and wallets. Under these circumstances, email-only for rights-critical steps and deadlines was not reasonable.

49. Kroll's acts and omissions were the direct and proximate cause of Plaintiff's and class members' injuries. But for Kroll's security failures, email-only notice, refusal to send postal mail for the 130th Omnibus Objection deadlines and tax-form deadline, and the broken, gated portal, Plaintiff and many class members would have timely started and completed verification and submitted tax forms; would not have had claims expunged or placed "on hold" thereby delaying plan distributions; and would have avoided phishing losses and mitigation costs.

50. Plaintiff and the Classes suffered damages including, without limitation: (a) phishing/crypto losses (for Plaintiff 1.9 ETH drained minutes after receipt); (b) time-value damages from distribution delays caused by email-only noticing and the portal's defects; (c) claim expungement/forfeiture tied to missed verification/tax-form deadlines; (d) out-of-pocket expenses (monitoring, device/wallet hardening, document procurement) and lost time; and (e) diminished privacy and ongoing identity and asset theft.

51. Plaintiff and the Classes seek compensatory and consequential damages in an amount to be proven at trial, together with pre- and post-judgment interest.

COUNT II

Texas Deceptive Trade Practices—Consumer Protection Act

(Tex. Bus. & Com. Code § 17.41 et seq.)

52. Plaintiff is a consumer under Tex. Bus. & Com. Code §17.45(4) because he sought and used services—the Kroll claims administration and creditor-facing services purchased for Plaintiff's benefit by the FTX Debtors/FTX Recovery Trust—and those services were provided to Plaintiff to allow him to assert and receive distributions on his claim.

53. Kroll engaged in deceptive acts, including: (1) representing services had characteristics/benefits they did not—namely, that no sensitive PII (e.g., full name, mailing address, date of birth, wallet / transaction details) was taken and that email processes were safe post-breach; (2) failing to disclose information known at the time of the transactions (that sensitive PII was in

"unstructured data"; that impersonation/email-change takeovers were active) to induce claimants to continue the email-only workflow; and (3) representing rights/obligations under the claims process that they did not have—implying email notice alone was reasonable and sufficient for rights-critical deadlines.

54. In the wake of a known security incident and live phishing campaign, persisting with email-only notice for rights-critical deadlines and omitting a postal backstop and manual tax-form submission channel was an unconscionable course of action that took grossly unfair advantage of claimants' lack of knowledge and inability to protect themselves.

55. Kroll's DTPA violations were producing cause of Plaintiff's damages, including (i) the 1.9 ETH theft after phishing, (ii) time-value/distribution harms from blocked verification and tax-form submission, and (iii) mitigation costs and loss of privacy/control of PII.

56. Kroll acted knowingly, and in some respects intentionally: it knew from its own investigations in other estates (e.g., BlockFi) that sensitive PII existed in "unstructured data," yet told claimants otherwise and failed to adjust notice and workflows accordingly.

57. Plaintiff seeks economic damages, attorneys' fees, costs, and treble damages for knowingly/intentional violations under the Texas DTPA.

58. Plaintiff has sent or is contemporaneously sending the pre-suit notice. To the extent notice was not feasible because of imminent limitations and the need for injunctive relief, Plaintiff requests the Court abate the DTPA claim for 60 days from service to allow cure discussions as provided by statute.

COUNT III

New York Unfair Deceptive Acts (in the alternative)

59. Kroll engaged in consumer-oriented deceptive acts and practices, including sending deceptive public-facing case notices and claimant communications, downplaying the breach (stating

no sensitive PII), failing to disclose material facts (PII present in files and in "unstructured data"; active impersonation), and encouraging continued email-only communications in a live phishing environment. These acts were misleading in a material way and injured Plaintiff. Plaintiff seeks actual damages, statutory damages, reasonable attorneys' fees, and injunctive relief under New York General Business Law §§ 349(h) and 350-e.

COUNT IV

Gross Negligence

60. Kroll's conduct was more than ordinary negligence. Knowing claimant PII had been exposed, and knowing claimants were being actively phished, Kroll consciously persisted in email-only, link-heavy, look-alike-prone messaging for rights-affecting deadlines; refused to switch to postal mail at scale even though it had the ability and had used mail for other critical communications; and continued to gate tax-form submission behind an unreliable claims portal that repeatedly flipped users back and forth between "Verified" and "On Hold" without explanation—even after third-party intelligence documented ongoing impersonation, email-change takeovers, and laundering routes using claimant data.

61. Kroll's failure to deploy obvious safeguards—First-Class Mail for rights-critical notices, mailed confirmations of status changes, a manual non-gated tax-form path, change-control hardening (mailed codes to the existing address; cooling-off periods; manual review of switches to recently created ProtonMail accounts), and dark-web monitoring—was an extreme departure from ordinary care in the face of a high likelihood of serious harm to a population whose PII was sealed precisely to avoid phishing and physical targeting.

62. Kroll's grossly negligent conduct was a substantial factor in causing Plaintiff's and the Classes' injuries and supports an award of punitive damages to punish and deter similar misconduct.

63. Plaintiff and the Classes seek punitive damages in an amount sufficient to reflect the reprehensibility of Kroll's conduct and to deter future violations.

COUNT V

Breach of Implied Contract (Privacy & Claims Administration)

64. By soliciting and accepting Plaintiff's and class members' PII and claim submissions and by requiring them to use the FTX Portal (KYC/review) and Kroll's EPOC (claim filing) to participate in the bankruptcy claims process, Kroll entered into implied contracts to (a) safeguard that information with reasonable security, (b) administer verification and tax-form steps with reasonable care, and (c) provide channels reasonably designed to ensure claimants could complete rights-affecting steps.

65. Plaintiff and class members performed by supplying accurate information and following Kroll's instructions. They reasonably expected Kroll would protect their data and provide a functional, safe process to complete verification and upload tax forms.

66. Kroll breached these implied promises by allowing unauthorized access to claimant data; by continuing to use email-only notices in a known phishing environment; by persisting in a defective, gated workflow without an alternative path; and by failing to provide a manual, non-gated submission option or mailed confirmations for rights-affecting status changes.

67. As a direct and proximate result, Plaintiff and class members suffered the damages described above, including phishing loss, time-value and distribution harms, and out-of-pocket costs.

68. Plaintiff and the Classes seek damages, restitution, and all other appropriate relief for Kroll's breach of implied contract.

COUNT VI

Negligent Undertaking (Restatement (Second) of Torts § 324A)

69. Kroll undertook to render services it knew were necessary for the protection of Plaintiff and the Classes—namely, safeguarding claimant PII and administering the verification/tax-form workflow and rights-affecting notices.

70. Kroll performed that undertaking negligently by using email-only notice post-breach; declining to send postal mail for the 130th Omnibus Objection deadlines and tax-form deadline; gating tax-form submission behind an unreliable, status-gated workflow; and failing to provide an alternative path or mailed confirmations.

71. Kroll's negligent performance increased the risk of harm to Plaintiff and class members (missed or ignored notices, status-flip lockouts, phishing) and was a substantial factor in the resulting losses.

72. Plaintiff and many class members relied on Kroll's undertaking—using the FTX Portal and Kroll's claimant communications/EPOC as instructed and foregoing other steps because Kroll was the exclusive channel for verification and claim administration.

73. Plaintiff and the Classes are entitled to damages proximately caused by Kroll's negligent undertaking.

COUNT VII

Negligent Post-Breach Notice and Claims Processing

74. After the August 19, 2023 incident, Kroll had a heightened duty to mitigate foreseeable harms and to provide notice and process accommodations reasonably calculated to reach claimants and enable timely compliance with rights-affecting steps.

75. Kroll breached that duty by continuing to rely on email-only notice—despite pervasive phishing and spam-filtering directed at Kroll-look-alike emails—and by failing to switch to postal mail for the most consequential communications, including the FTX 130th Omnibus Objection deadlines (to commence by March 1, 2025 and complete by June 1, 2025) and the tax-

form deadline. The confirmed plan did not contain fixed dates in the plan text; therefore, Kroll's channel choice made those notices outcome-determinative. Many reasonable claimants did not open Kroll emails because doing so felt like "Russian roulette" during active phishing campaigns; many notices landed in junk/spam folders and went unseen.

76. Independently, FTX operated a portal that blocked W-9/W-8BEN submission unless "KYC Verified," yet the system erroneously flipped verified users back to "On Hold/Unverified," with no manual override, no mailed confirmation of status changes, and no alternative submission path—guaranteeing preventable non-compliance.

77. Kroll's support communications compounded these failures—issuing boilerplate "try again" and "fixed" messages, redirecting claimants to other inboxes, and providing no durable fix—while the expungement and tax-form deadlines approached.

78. Kroll misrepresented that sensitive PII was not implicated and later acknowledged dates of birth in "unstructured data" in another crypto estate (BlockFi), thereby reducing vigilance and increasing phishing success.

79. As a direct and proximate result of Kroll's negligent notice and claims processing, Plaintiff and class members missed or were unable to complete verification and tax-form requirements they otherwise would have satisfied, suffered phishing losses, and incurred time-value and administrative damages.

80. Plaintiff and the Classes seek damages for these injuries and a declaration that Kroll's post-breach notice/processing practices were unreasonable and unlawful under the circumstances.

81. Plaintiff and the Classes further seek injunctive relief requiring multi-channel notice (email and first-class mail with typed URLs/unique codes), mailed confirmations for any rights-affecting status change, defined cure windows before expungement, and a manual/alternative channel for verification and tax-form submission. Kroll continues to administer creditor-facing

communications and records relating to these estates, so the risk of future injury is ongoing absent court-ordered safeguards.

COUNT VIII

Negligent Misrepresentation (post-breach process statements)

82. Kroll, in post-breach communications, represented that verification errors were "fixed," that claimants should "try again," or that status was "Verified," when the system continued to revert to On Hold/Unverified and block tax-form submission. Kroll's role as the court-appointed claims/noticing agent and Administrative Advisor placed it in a position of unique and trusted access to creditor information and process control, creating a special relationship sufficient to support negligent-misrepresentation liability.

83. Kroll supplied this information in the course of its professional administration duties and failed to exercise reasonable care. Plaintiff and class members justifiably relied by continuing with the same broken workflow and forgoing escalation alternatives, causing missed deadlines, time-value losses, and expungement.

84. Plaintiff seeks damages proximately caused by this reliance.

COUNT IX

Unjust Enrichment (in the alternative)

85. Kroll received substantial compensation for serving as noticing/claims agent and Administrative Advisor across the crypto estates while externalizing the costs and risks of its deficient security and post-breach administration into claimants.

86. It would be inequitable for Kroll to retain those benefits without reimbursing the losses it caused and without funding remedial measures (including monitoring, security improvements, re-noticing, and re-opened submission windows).

87. Plaintiff pleads unjust enrichment in the alternative to his contract and tort claims to the extent the Court finds no enforceable contract governs Kroll's duties to claimants.

88. Plaintiff and the Classes seek restitution and disgorgement of ill-gotten benefits and fee offsets commensurate with the harms caused.

COUNT X

Declaratory and Injunctive Relief (28 U.S.C. §§ 2201-02)

89. An actual, justiciable controversy exists concerning Kroll's ongoing obligations to secure claimant data, to give adequate notice of rights-affecting steps, and to operate a functional verification/tax-form process that does not arbitrarily block compliant claimants.

90. Plaintiff seeks a declaration that Kroll's post-breach email-only noticing and gated portal were unreasonable under the circumstances and that Kroll must employ processes reasonably calculated to reach and protect claimants going forward.

91. Plaintiff also seeks a permanent injunction requiring Kroll, for no less than three (3) years, to implement: (a) multi-channel notice (email and First-Class Mail) for any rights-affecting deadline, with typed URLs/unique access codes and no clickable links; (b) mailed confirmations of any verification status change and a minimum 30-day cure window before expungement or forfeiture; (c) change-control hardening: mailed one-time codes to the existing postal address before any email/phone change takes effect; (d) a 14-day cooling-off period for contact-method changes unless verified by a mailed code; (e) manual review of switches to recently created ProtonMail or other high-risk domains; (f) a manual/alternative method to complete verification and to submit W-9/W-8BEN that is not gated by portal flags, with a published escalation SLA (5 business-day escalation; 10 business-day resolution); (g) immutable audit logs of status changes and a human-review override; (h) industry-standard deliverability and anti-spoofing controls (dedicated domains, DMARC/SPF/DKIM enforcement, link-tracking discipline, look-alike-domain takedowns keyed to

FTX/Kroll/claims keywords); (i) independent annual audits of security, deliverability, and portal workflow with reports available to the Court; and (j) funded credit/ID and crypto-account monitoring and a phishing loss reimbursement program for affected claimants.

92. The requested relief will prevent future harms that damages alone cannot remedy, will ensure fair access to distributions, and will align Kroll's practices with the foreseeable risks unique to crypto creditors.

93. Plaintiff and the Classes lack an adequate remedy at law for the prospective injuries addressed by the requested injunctions; monetary relief cannot ensure timely, safe, and effective administration of ongoing claimant obligations.

94. The balance of equities and the public interest favor injunctive relief because it protects thousands of claimants' rights to be heard and to receive distributions without undue risk of fraud or expungement caused by defective processes.

95. Plaintiff and the Classes also seek their reasonable attorneys' fees and costs to the extent permitted by law, including under common-fund/common-benefit doctrines and the Court's equitable powers.

ARBITRATION/CLASS-ACTION WAIVER

96. The FTX Portal is not Kroll's "Site" as defined in Kroll's Terms of Use. Plaintiff did not assent in the FTX Portal to any Kroll Terms. The FTX Portal contained an FTX data-processing consent only; it displayed no Kroll Terms, no arbitration, and no class waiver. To the extent Kroll points to a separate click-through on its EPOC or Kroll Site, the clause is narrow and elective, applying only to disputes "arising out of or relating to these Terms or our Site," and there is no delegation clause—so this Court decides arbitrability. Plaintiff's claims arise from Kroll's court-appointed administration and data-security duties (M365 breach; post-breach notice channels; lack of a non-gated tax-form path), which exist independently of any website use and fall outside of any

site-limited clause. Alternatively, extracting arbitration/class waiver as a condition to filing a federal Form 410 is procedurally unconscionable; and under New York public policy, gross negligence cannot be contractually excused. The Terms' "individual basis" language is cabined to arbitration; there is no stand-alone class waiver in court. The Plan's Kroll Security-Incident carve-out confirms these are independent third-party tort claims contemplated to proceed 'in another proceeding,' undermining any non-signatory theory.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Classes;

B. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

C. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

D. For an award of punitive damages, as allowed by law;

E. Texas DTPA Remedies: economic damages, treble damages for knowing/intentional violations, and reasonable and necessary attorneys' fees (DTPA § 17.50(d));

F. New York GBL §§ 349/350 (alternative): statutory damages and attorneys' fees;

G. For an award of attorneys' fees and costs, and other expenses, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

Dated: August 19, 2025

Respectfully submitted,

HALL ATTORNEYS, P.C.

By: */s/ Nicholas Andrew Hall*

Nicholas Andrew Hall
State Bar No. 24069863
nhall@hallattorneys.com
P.O. Box 1370
Edna, Texas 77957
+1 713 428 8967

ATTORNEY FOR PLAINTIFF AND PUTATIVE CLASSES