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

JOHN DOE 1, JOHN DOE 2, and JANE DOE 1, individually and on behalf of all others similarly situated,	**Case No.: 1:25-cv-01319-RP**
Plaintiffs,	**CLASS ACTION COMPLAINT**
v.	
KROLL RESTRUCTURING ADMINISTRATION LLC (f/k/a Prime Clerk LLC),	**JURY TRIAL DEMANDED**
Defendant.	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs John Doe 1, John Doe 2, and Jane Doe 1 (collectively, "Representative Plaintiffs" or "Plaintiffs"), individually and on behalf of the classes/subclasses as also defined herein of similarly situated persons, allege the following against Kroll Restructuring Administration LLC (f/k/a Prime Clerk LLC) ("Kroll" or "Defendant"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, Plaintiffs specifically alleges as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Kroll for two failures: (1) a security failure—an August 2023 SIM swap of a Kroll employee's mobile number enabled access to claimant files containing names, mailing addresses, email addresses, and account/claim information (the "Security Incident")—and (2) a post-incident administration failure—Kroll

continued to rely on a contaminated email channel and fragile portal workflows for rights-critical notices amid active impersonation of Kroll/estate communications.

2. Plaintiffs and the class members suffered: (i) Security Incident exposure (out-of-pocket mitigation, time spent responding, and ongoing risk), (ii) phishing/targeted-attack losses (e.g., wallet drains from Kroll/estate themed "distribution" lures and portal impostors), and (iii) bankruptcy process losses (expungements, forfeitures, and distribution delays producing time-value losses).

3. Plaintiffs seek damages and narrow injunctive relief (USPS backstops; authenticity cues and phishing exemplars; email sender authentications and fast lookalike domain takedowns; translations; portal/help desk SLAs) funded by Kroll so that creditor distributions are not reduced.

PARTIES

4. Plaintiff John Doe 1 is a Texas resident and FTX scheduled creditor. He began receiving Kroll/estate themed phishing on or around September 2023. On or around November 2023, his FTX portal claim status changed from "Verified" to "Unverified" without explanation, blocking tax-form submission and delaying distributions, causing time-value loss and mitigation time.

5. Plaintiff John Doe 2 is a Texas resident and BlockFi scheduled creditor. He used the BlockFi "Scheduled Information" workflow without any "I agree" clickwrap or conspicuous Terms. On or about August 26, 2025, after receiving a Kroll/estate branded "distribution" email, he connected a wallet to a spoofed site with a Kroll branded URL and was drained of approximately $300,000. He submitted an FBI report the same day and retained transactional records.

6. Plaintiff Jane Doe 1 is a Texas resident and FTX scheduled creditor. Her claim was expunged on April 2, 2025 after portal-gated steps were not completed. On September 26, 2025, Kroll confirmed a phishing email to her, forwarded an internal response thread, and misdirected her to BlockFi support (the wrong estate).

7. Defendant Kroll is a Delaware LLC headquartered in New York, New York with offices in Texas. It serves as claims and noticing agent (28 U.S.C. § 156(c)) and Administrative Advisor (11 U.S.C. § 327) in the FTX, BlockFi, and Genesis Chapter 11 Cases.

JURISDICTION AND VENUE

8. This Court has jurisdiction under 28 U.S.C. §§ 1331, 1332(d), and 1367. The amount in controversy for the class exceeds $5,000,000 exclusive of interest and costs, and at least one class member is a citizen of a different state from Defendant.

9. Venue is proper under 28 U.S.C. § 1391 because a substantial part of the events or omissions occurred in this District and/or Kroll is subject to personal jurisdiction here.

10. Not court-compelled acts. The conduct challenged here—security configuration, scope and timing of post-incident review, noticing channel design, and portal/support workflows—was not commanded by any court order, nor does the relief requested herein interfere with post-confirmation administration or the quantum of distributions to creditors in the bankruptcy cases.

FACTUAL ALLEGATIONS

A. Kroll's Court-Appointed Functions and the Duties That Flow From Them

11. Kroll acted in two capacities that carry distinct but overlapping obligations in FTX, BlockFi, and Genesis: (1) as claims and noticing agent under 28 U.S.C. § 156(c) to perform clerk-type tasks ("Claims Agent"); and (2) as Administrative Advisor under 11 U.S.C. § 327 to provide professional services beyond the clerk's scope.

12. As Claims Agent, Kroll functioned as an officer of the court to perform tasks the clerk would otherwise perform, including servicing bar date and other notices under Bankruptcy Rules 2002 and 3003; maintaining the mailing matrix and claims register; processing proofs of claim; and complying with sealing, redaction, and protective order requirements governing creditor PII. From these sources, Kroll owed duties to execute the notice program as ordered and, consistent with due process principles, to implement service that is reasonably calculated under the circumstances to apprise known creditors of rights-affecting events.

13. Separately, in its Administrative Advisor function, Kroll was retained to perform non-clerk work: advising the bankruptcy estates on creditor legal noticing and communications (and thereby established the requisite standards for court noticing), secure data room administration, assistance with schedules/SOFAs, claims verification and reconciliation workflows, plan solicitation and balloting, portal design and operation, and distribution implementation. As an estate professional, Kroll owed a high standard of care, candor, and disinterestedness to the estates for the benefit of the creditor body, including the obligation to design and operate these programs in a manner that affords creditors a meaningful opportunity to receive, understand, and act on rights-critical information.

14. The section 156(c) noticing orders and section 327 retention orders afforded Kroll discretion to design operational details (security, communications, portal/help desk). No court order mandated "email-only" for rights-critical notices under active impersonation conditions, nor barred USPS backstops, translations, or publication of phishing exemplars on the docket with authenticity cues to creditors.

15. The bankruptcy court sealing and redaction orders, together with Bankruptcy Rule 9037, required Kroll to segregate, restrict, and safeguard customer-creditor information; to limit

access and transmission to what the orders permit; and to handle protected data using procedures consistent with those orders and with applicable professional standards.

16. Nothing in the noticing or sealing orders mandated email-only service under known spoofing conditions or barred Kroll from: (a) adding USPS First-Class Mail to defined cohorts, (b) publishing phishing exemplars on the docket and authenticity cues on case sites, (c) implementing hardened/bank-grade messaging, (d) providing translations for non-English speaking cohorts, or (e) setting portal/support SLAs that prevent silent claim-status changes and provide individualized explanations.

17. Kroll's approved retention agreements and the orders authorizing those engagements required it to perform services in accordance with the Bankruptcy Code and Rules, court orders, local protocols, and professional standards of care. Because those services were undertaken for the benefit of the creditor body, Kroll's performance had to be consistent with protecting creditor rights and ensuring the integrity of notice, claims administration, and distributions.

18. Independent of bankruptcy law, Kroll's collection and processing of creditor PII triggered obligations under generally applicable data privacy and consumer protection statutes to maintain reasonable administrative, technical, and physical safeguards, to provide accurate and timely information about security matters, and to avoid misleading communications about the authenticity or source of creditor-facing messaging.

B. Court Sealing and Redaction Regimes: Scope, Rationale, and Judicial Findings

19. The bankruptcy courts entered orders to protect customer-creditors against crypto-related crimes by authorizing redaction and sealing of PII—including, at minimum, names,

physical addresses, email addresses, claim/account information—across public filings such as creditor matrices, schedules/SOFAs, claims registers, proofs of claim, and service affidavits.

20. Courts grounded these protections to protect customer-creditors under 11 U.S.C. § 107(c) (undue risk of identity theft or unlawful injury), together with Bankruptcy Rule 9037 and applicable local protocols. See*, e.g., Committee Joinder & Brief, In re FTX Trading, Ltd.*, No. 22-11068, Dkt. 408 (Bankr. D. Del. Jan. 8, 2023) (quoting Collier that § 107(c) of the Bankruptcy Code gives "broad discretion" to protect identifying information where disclosure creates undue risk of identity theft or unlawful injury to the individual or individual's property).

21. In FTX, Judge Dorsey credited uncontroverted evidence that under § 107(c) "customers can be identified just by a name" in an era of open-source intelligence and the dark web. Hon. John T. Dorsey, *In re FTX Trading, Ltd.*, No. 22-11068 (Bankr. D. Del. June 12, 2023) (June 9, 2023 Hr'g Tr. at 157:16–21). Most pointedly: "It's the customers that are the most important issue here. I want to make sure that they are protected and they don't fall victim to any types of scams that might be happening out there." Id. at 157:16–21.

22. Similarly in *In re Genesis Global Holdco, LLC, et al.*, No. 23-10063, Dkt. 581 (Bankr. S.D.N.Y. Aug. 4, 2023) *Memorandum of Decision*, Judge Lane similarly granted redaction of customer information (including email addresses), holding that "[t]he publication of names alone has been found to heighten the risk of identity theft," and noting a record "replete with examples of past harassment, threats, and attacks against individuals motivated by the theft of cryptocurrency." *Id.* at 29, 31.

23. The BlockFi court record collected crypto bankruptcy court rulings and articulated why sealing is absolutely essential to protecting creditors, stressing that disclosure of names alone can precipitate identity theft, verbal and physical harassment, theft and/or robbery, and hacking—

risks magnified for crypto because transactions are irreversible. *In re BlockFi Inc.*, No. 22-19361, Dkt. 581 (Bankr. D.N.J. Jan. 10, 2023) (Official Committee Joinder & Galka Decl. excerpts).

24. The confidentiality orders suppressed PII while preserving service to customers at their actual physical and email addresses, confirming that postal mail remained practicable and consistent with sealing whenever electronic reliability was impaired.

C. The Security Incident and Kroll's Failure to Adapt Creditor Noticing and Workflows

25. On or about August 19, 2023, a threat actor SIM swapped a Kroll employee's mobile number and used that vector to access court sealed and redacted customer-creditor information in Kroll's M365 cloud environment. Kroll's incident notice in FTX states that the attacker accessed files containing names, physical addresses, email addresses, and account information and warned that the data could be used for phishing emails.

26. The incident here began with the very failure mode Kroll had identified over a year before—a SIM swap attack and not password protecting files at rest. Before August 2023, Kroll publicly advised against using SMS/telephone for MFA because it is susceptible to SIM swap attacks and recommended that organizations use phishing-resistant methods—"do not allow … telephone call or SMS text" MFA; instead allow TOTP app codes or a physical token.[1] Kroll likewise advised organizations to password protect files in transit and at rest, calling encryption "your last line of defense," and to ensure an encryption policy covers all portable IT assets.[2]

27. Although the compromise occurred in August 2023, Kroll did not review "Unstructured Files" for over three months; when finally reviewed (including in BlockFi), those

[1] Kroll, *MFA Prompt Bombing No More: Countering MFA Bypass Tactics* (May 23, 2022), https://www.kroll.com/en/publications/cyber/mfa-prompt-bombing-no-more.
[2] Ryan Spelman, *Six Key Questions to Ask Outside Counsel About Their Cyber Security Posture* (Oct. 16, 2019), https://www.kroll.com/en/publications/cyber/six-key-questions-outside-counsel-cyber-security-posture.

files contained dates of birth and driver's license numbers—sensitive PII far beyond routine contact data or information provided by customer-creditors on claim submissions.[3]

28. The FTX estate professionals likewise recorded review of a "Kroll spreadsheet involving FTX claimant dates of birth" and lookalike domains (e.g., "portal-ftx.com" and "withdrawal.kroll-ftx.com"). *See* Monthly Fee Statement of Sullivan & Cromwell LLP for Oct. 2023 (Cyber Issues category), *In re FTX Trading, Ltd.*, No. 22-11068, Dkt. 4424-2 (Bankr. D. Del. filed Nov. 30, 2023).

29. Independent intelligence reports contemporaneous with the Security Incident documented customer-creditor PII offered for sale on the dark web and fake portals engineered to mimic Kroll/estate communications.[4]

30. The FTX estate publicly froze affected portal accounts "in response to Kroll's cybersecurity incident" and warned customers to be on high alert.[5] Separately, the United States Trustee catalogued more than $1.29 million in professional time addressing "Cyber Issues" in FTX and reserved rights as to whether Kroll—not the estate—should bear those costs. *See U.S. Trustee's Reservation of Rights Regarding Professional Fees Related to the Kroll Security Incident*, *In re FTX Trading, Ltd.*, No. 22-11068, Dkt. 9317 (Bankr. D. Del. Mar. 14, 2024).

31. Notwithstanding these conditions, Kroll continued email-only noticing without promptly deploying: (a) USPS backstops to defined cohorts for all rights-critical notices; (b) public authenticity cues (exemplar screenshots; domain-validation instructions), (c) translations for major

[3] Letter from the Official Comm. of Unsecured Creditors of BlockFi Inc. to State Attorneys General re Kroll Security Incident (Jan. 2024) (https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-1033.pdf).
[4] Inca Digital, *Crypto Threat Intelligence Alert FTX Debt Claims* 9–11 (2023) (*https://drive.google.com/file/d/1fokAk1ZrnNirpd1FwL3l4LApMYVEz5xC/view*).
[5] See FTX Official (@FTX_Official), Post to X (Aug. 25, 2023, 5:12 PM).

non-English language cohorts, (d) portal/support SLAs to prevent silent claim-status changes and provide individualized explanations.

32. Postal mail was practicable under the confidentiality orders and would have been reasonably calculated under the circumstances to reach creditors given that the email channel was severely compromised and unsafe.

33. The bankruptcy courts did not give Kroll releases or exculpation from third-party claims for damages related to the Security Incident. The FTX confirmation order preserves customer-creditor claims against Kroll and clarifies that those damages recoverable in another proceeding are not capped by plan distributions. The BlockFi confirmation order likewise preserves customer-creditor claims against Kroll in law or in equity related to the data breach. The United States Trustee also reserved that estates should not bear ultimate responsibility for the Security Incident costs.

34. The FTX court subsequently reduced the Disputed Claims Reserve by approximately $360 million for customer-creditor claim expungements for failures to complete rights-critical steps, indicating large cohorts with bankruptcy process losses who failed portal-gated workflows due to the Security Incident.

35. The full scope of the Security Incident was not reasonably discoverable by Plaintiffs until Kroll later disclosed that it had not reviewed "Unstructured Files" for months and that those files contained dates of birth and driver's license numbers; phishing/impersonation waves and portal freezes/lockouts then unfolded in the months that followed. Plaintiffs allege (i) the discovery rule: they could not reasonably discover the nature and extent of Kroll's Security Incident failures and post-incident administration until Kroll's later disclosures and estate actions; (ii) fraudulent concealment: Kroll omitted material facts needed to understand the nature and scope

of impacted repositories/fields and the program changes required to protect known creditors; and (iii) equitable tolling during periods of concealment and continuing violation.

CLASS ALLEGATIONS

36. Plaintiffs bring this action under Rules 23(a), 23(b)(2), and 23(b)(3) on behalf of the following classes and subclasses, reserving the right to refine at certification:

37. **Nationwide Security Incident Exposure Class**. All natural-person customers/creditors whose PII in Kroll's custody for the FTX and/or BlockFi Chapter 11 Cases was exposed or accessed in or after the August 19, 2023 security incident. The class period begins on or about August 19, 2023 and continues through the date of class certification.

38. **Targeted Attack/Phishing Damages Subclass**. Class members who suffered monetary loss or other concrete harms induced by Kroll/estate themed messages or portals (e.g., wallet drains from distribution lures or portal impostures). The class period begins on or about August 19, 2023 and continues through the date of class certification.

39. **Bankruptcy Process Loss Subclass.** Class members who suffered, expunged, forfeited, or delated distributions/allowance where rights-critical steps (e.g., customer-creditor KYC/verification, tax-form submission) were noticed through a compromised email channel amid active impersonation and portal instability. The class period begins on or about August 19, 2023 and continues through the date of class certification.

40. Class membership is ascertainable from Kroll's claimant repositories and notice/portal logs (including affected account lists, bounce reports, lockouts, status transitions, and help desk records). Common issues predominate because Kroll's security configuration, scoping timeline, and post-incident communications design were uniform program decisions.

41. The class members number in the hundreds of thousands, if not millions, making joinder impracticable. Common questions predominate, including: whether Kroll's security controls and post-incident communications design were reasonable under the circumstances; whether Kroll should have supplemented email notices with first class mail to defined cohorts; and whether Kroll's conduct caused phishing losses and/or bankruptcy process harms.

42. Plaintiffs' claims are typical. Plaintiffs will fairly and adequately protect the Classes' interests with qualified counsel.

43. Certification is proper under Rule 23(a), (b)(2), and (b)(3).

CLAIMS FOR RELIEF

COUNT I — WILLFUL MISCONDUCT/RECKLESSNESS

44. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

45. Kroll controlled privileged access to claimant repositories and creditor-facing channels and knew, before August 2023, that SMS-based MFA is vulnerable to SIM swap and should be replaced by TOTP/hardware tokens, and that encryption at rest is a last line of defense.

46. After the SIM swap enabled access to claimant files containing names, addresses, emails, claim/account information, and other sensitive data, Kroll itself warned the data could be used for phishing emails.

47. Kroll deliberately did not review "Unstructured Files" for over three months; when finally reviewed (including in BlockFi), those files contained dates of birth and driver's license numbers—PII requiring heightened protections and disclosures.

48. Independent intelligence reports documented sale of FTX debt-claims data and fake portals; the FTX estate froze affected portal accounts, locking out customer-creditors, and warned customers to be on high alert for attacks.

49. Despite actual knowledge of ongoing impersonation, Kroll deliberately continued email-only direction to Kroll/estate branded sites/emails, steering victims back into the same look-and-feel that phishers were spoofing—without timely USPS backstops, authenticity cues and exemplars, translations for major cohorts, strict SPF/DKIM/DMARC enforcement, or rapid lookalike domain takedowns.

50. Kroll's deliberate choices magnified foreseeable harms to Representative Plaintiffs and class members. Kroll's choices foreseeably exposed class members to wallet-drain lures (e.g., the $300,000 BlockFi loss to John Doe 2), status toggles (e.g., Verified to Unverified for John Doe 1), and deadline failures amid confusion (e.g., expunged FTX claim for Jane Doe 1).

51. Kroll deliberately failed to publish side-by-side "legitimate vs. spoof" cues and failed to provide translations for major non-English language cohorts, despite the global creditor base and known phishing.

52. Kroll communications deliberately steered victims to Kroll websites to verify inbound emails, confusing class members as phishers spoofed Kroll branding and domains.

53. The United States Trustee flagged invoices related to the Security Incident and reserved rights as to whether Kroll, not the FTX estate, should bear those costs—underscoring that Kroll's choices were its responsibility.

54. In light of Kroll's pre-incident guidance, post-incident knowledge, and months-long delay to review compromised files while impersonation continued, maintaining

email-only and failing to deploy basic mitigations like postal mail for rights-critical notices was reckless at minimum and willful in its disregard of known, substantial risks.

55. The conduct challenged—security configuration, scope and timing of post-incident review, channel design, and portal/help-desk workflows—was not commanded by any court order. The noticing orders did not require "email-only" notice or prohibit USPS backstops; sealing orders preserved the use of physical addresses for mailed service to known creditors.

56. Kroll owed independent duties to exercise reasonable care in safeguarding sealed/redacted PII and designing a post-incident communications program reasonably calculated to reach known creditors under the circumstances—duties arising from its court-approved roles, the confidentiality regime, and its professional undertaking to the estates for the benefit of creditors.

57. Kroll's willful misconduct and/or recklessness directly and proximately caused: (i) phishing/targeted-attack losses (including the $300,000 BlockFi wallet drain of John Doe 2), (ii) exposure and loss of control of PII with ongoing risk, (iii) mitigation/time costs, and (iv) bankruptcy process harms (expungements/forfeitures/delays and time-value losses for John Doe 1 and Jane Doe 2).

58. As a further result of the willful misconduct and/or recklessness of Kroll, the Plaintiffs and class members incurred out-of-pocket losses, time costs, emotional distress, and may be required in the future to obtain professional treatment for mental health counseling, as well as treatment for physical injuries, due to the disclosure of their identities to bad actors.

59. The full scope—including the "Unstructured Files" with DOB/driver's license data—emerged late 2023–early 2024; portal/account restrictions continued into 2025; bankruptcy process harms matured months to a year later and are continuing.

COUNT II — GROSS NEGLIGENCE

60. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

61. Kroll owed duties independent of contract to exercise reasonable care in safeguarding sealed/redacted PII and to design post-incident communications reasonably calculated to reach known creditors—duties arising from its court-approved roles, the confidentiality regime, and its professional undertaking to the estates for the benefit of creditors.

62. As a court-approved professional stewarding sealed/redacted PII and creditor communications, Kroll owed a duty of utmost care commensurate with its roles; Kroll's conduct was an extreme departure, including:

a. Allowing SMS-susceptible privileged access despite Kroll's own guidance counseling against SMS MFA and in favor of TOTP/hardware tokens and failing to ensure encryption at rest;

b. Failing for months to review "Unstructured Files," which later were found to contain DOB/driver's-license data—precisely the sort of PII that demands swift containment and notice;

c. Maintaining email-only communications to Kroll-branded web/email points amid active impersonation and a known portal freeze;

d. Not deploying USPS postal mail, authenticity cues and phishing exemplars, translations, strict SPF/DKIM/DMARC alignment, and rapid takedowns for lookalike domains—despite discretion to implement such measures;

e. Operating unstable portal workflows that silently toggled claim status and impeded tax-form submission, without individualized explanations;

f. Failing to provide timely, sufficiently granular detail about impacted repositories/fields so class members could mitigate; and

g. Directly and wantonly violated court orders of bankruptcy judges by not protecting court-ordered sealed/redacted PII and allowing it to be used to perpetrate the very crypto-related crimes that Kroll was warned about.

63. This combination—SIM swap susceptibility against Kroll's own guidance; a multi-month scoping delay as DOB/DL sat in Unstructured Files; and email-only communications amid impersonation and a portal freeze—was an extreme departure from the care required of a court-appointed professional stewarding sealed/redacted PII and rights-critical notices.

64. Kroll's gross negligence proximately caused: (a) phishing losses (e.g., $300,000 BlockFi phishing damages to John Doe 2), (b) exposure/ongoing risk, (c) mitigation/time costs, and (d) expungements/forfeitures and time-value losses (e.g., time-value losses of John Doe 1 and Jane Doe 1 expunged claim).

65. The full scope—including the "Unstructured Files" with DOB/driver's license data—emerged late 2023–early 2024; portal/account restrictions continued into 2025; bankruptcy process harms matured months to a year later and are continuing.

COUNT III — NEGLIGENCE

66. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

67. In the FTX, BlockFi, and Genesis cases, customer-creditor PII—including names, mailing addresses, email addresses, phone numbers, and claim/account information—was collected, maintained, and used by Kroll in connection with claims administration, noticing, verification, and distributions.

68. Kroll had full knowledge of the sensitivity of customer-creditor PII and the types of harm that would flow if this data were accessed or misused—including phishing, identity theft, and targeted "distribution" lures—as reflected in Kroll's own warnings to claimants that the exposed data could be used for phishing emails.

69. Before August 2023, Kroll publicly advised against SMS/phone-based MFA and recommended TOTP or hardware tokens for higher-risk access and emphasized encryption at rest for a last line of defense. Kroll knew—or should have known—that relying on SMS for privileged access created a material risk of SIM swap compromise.

70. Kroll owed a duty independent of contract to exercise reasonable care in safeguarding, securing, and protecting customer-creditor PII and related systems from unauthorized access and misuse. That duty included, at a minimum, designing, maintaining, and testing security protocols for privileged access and data at rest, consistent with Kroll's own published guidance and its role as a court-approved professional stewarding sealed/redacted PII.

71. Kroll owed a duty to have procedures to detect, contain, and prevent impersonation and spoofing, including: sender-authentication enforcement, lookalike domain takedowns, publication of phishing exemplars and authenticity cues, and translations for major language cohorts to ensure that notices were reasonably calculated to be understood by known creditors.

72. Once Kroll learned of the SIM swap and active impersonation, it owed a duty to adapt its notice/portal program—including deploying USPS backstops to defined cohorts (e.g., unverified/expunged; bounced-email; non-English recipients) and providing clear, individualized explanations for portal status changes—so known creditors would receive rights-critical information despite a contaminated email channel.

73. Kroll breached its duty by failing to implement phishing-resistant MFA for privileged access consistent with Kroll's own guidance; by failing to adequately encrypt/protect data at rest; and by otherwise failing to employ reasonable security to prevent the SIM-swap-enabled access to claimant files.

74. Kroll did not review "Unstructured Files" for over three months; when finally reviewed (including in BlockFi), those files contained dates of birth and driver's license numbers—sensitivities exceeding customer-creditor proof of claim data fields—prolonging exposure and impairing mitigation.

75. Despite a known contaminated email channel and the FTX portal freeze, Kroll continued email-only direction to Kroll/estate branded web/email points without promptly deploying USPS backstops, public authenticity cues and exemplars, translations for major language cohorts, sender-authentication enforcement with rapid lookalike domain takedowns, and portal/support SLAs that prevented silent claim-status changes and provided clear individualized explanations.

76. Kroll failed to provide timely, sufficiently granular disclosure of the repositories and fields compromised (including the "Unstructured Files" containing DOB/driver's license data), thereby delaying and impairing class members' ability to assess risk and mitigate harm.

77. Kroll's duties sound not only in its engagements and court orders but also in independent, generally applicable obligations that arise when an entity collects and controls sensitive personal data of known individuals for operational use.

78. The injury was reasonably foreseeable even if caused in part by criminal actors: Kroll itself warned of phishing, public intelligence reports documented sale of FTX debt-claims data and fake portals, and the estate froze affected accounts because of the Kroll incident.

79. Kroll knew (and its own publications emphasize) that phishing is a dominant threat vector and that crypto-customer PII would be targeted for "distribution" lures.

80. Once Kroll possessed the PII and controlled the notice/portal program, class members lacked the ability to secure it or to control the channels through which rights-critical notices would be delivered.

81. Kroll controlled security architecture; selected/operated channels; and was positioned—by orders and engagement—to supplement electronic notice with USPS First-Class Mail when electronic reliability was impaired.

82. But for Kroll's security failures and unreasonable post-incident program design, Plaintiffs' and class members' PII would not have been accessed; phishing lures would have been mitigated with authenticity cues, translations, and takedowns; and rights-critical steps would have been reasonably communicated using reliable channels, preventing wallet drains and claim expungements/forfeitures/time-value losses.

83. As a direct and proximate result of Kroll's negligence, Plaintiffs and class members have suffered and will suffer injuries including, without limitation:

a. Phishing/targeted-attack losses (e.g., the $300,000 wallet drain to John Doe 2 following a Kroll/BlockFi themed "distribution" lure);

b. Loss of control over how their PII is used;

c. Compromise and exposure of PII, with ongoing risk;

d. Out-of-pocket mitigation (monitoring, security tools) and time spent responding;

e. Time-value and other bankruptcy process harms (delayed distributions; expungements/forfeitures where rights-critical steps were not reasonably communicated);

f. Reputational, anxiety, and emotional distress harms; and

g. The diminished value of Kroll's administrative services delivered to the estates and their customers.

84. The full scope of impacted repositories was not disclosed until late 2023–early 2024 (including the "Unstructured Files" review identifying DOB/driver's license data), and portal/account measures continue into 2025. Bankruptcy process injuries matured as rights-critical steps went uncompleted amid the contaminated channel and portal instability.

COUNT IV — NEGLIGENT UNDERTAKING

85. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

86. Kroll undertook to render services to the estates and their customer-creditors necessary for creditors to receive and act upon rights-critical information.

87. Kroll assumed responsibility and owed duties independent of contract to exercise reasonable care in: (a) collecting and safeguarding sealed/redacted PII; (b) designing/operating email, web, and portal channels; (c) configuring privileged access security; (d) implementing workflows for verification, tax forms, and claim reconciliation; and (e) coordinating content and cadence with estate professionals for the benefit of creditors.

88. Creditors reasonably relied on Kroll's performance of this undertaking as the official channel to receive and act on rights-critical information.

89. Kroll's actions/omissions increased risk: SIM-swap-susceptible access, email-only amid active impersonation, lack of authenticity cues, lack of translations, no USPS backstops, unstable portal workflows, and delayed and/or unresponsive responses to customer-creditor support inquiries.

90. Kroll failed to implement phishing-resistant MFA; to timely review "Unstructured Files"; to deploy USPS backstops, authenticity cues, translations, sender-auth enforcement, and

rapid takedowns; or to maintain portal/support SLAs that ensured stability and individualized explanations.

91. Kroll's negligent undertaking was a but-for and proximate cause of phishing losses, exposure/ongoing risk, mitigation/time costs, and bankruptcy process harms.

92. Kroll's negligent undertaking directly and proximately caused: (i) phishing/targeted-attack losses (including the John Doe 1 $300,000 BlockFi wallet drain), (ii) exposure and loss of control of PII with ongoing risk, (iii) mitigation/time costs, and (iv) bankruptcy process harms (expungements/forfeitures/delays and time-value losses).

93. As a further result of the negligent undertaking of Kroll, the Plaintiffs and class members incurred out-of-pocket losses, time costs, emotional distress, and may be required in the future to obtain professional treatment for mental health counseling, as well as treatment for physical injuries, due to the disclosure of their identities to bad actors.

94. The full scope—including the "Unstructured Files" with DOB/driver's license data—emerged late 2023–early 2024; portal/account restrictions continued into 2025; bankruptcy process harms matured months after the Security Incident and are ongoing.

COUNT V — BREACH OF FIDUCIARY DUTY

95. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

96. As Administrative Advisor under 11 U.S.C. § 327, Kroll was a court-approved professional person with duties of undivided loyalty, candor, and care to the estate for the benefit of the creditor body. As claims and noticing agent under 28 U.S.C. § 156(c), Kroll functioned as an officer of the court charged with faithfully executing court-approved noticing, claims administration, and confidentiality obligations for the protection of known creditors.

97. Kroll owed fiduciary duties to: (a) implement reasonable security for sealed/redacted PII; (b) timely, accurately, and fully inform the estates and the bankruptcy courts about the nature/scope of compromise and remediation; (c) design and execute a communications program reasonably calculated to reach known creditors under the conditions that existed post-Security Incident; (d) avoid self-serving steering that would prejudice creditors' rights (e.g., to its site Terms/arbitration); and (e) eschew concealment or minimization of operational risks that would impair known creditors' ability to protect their claims.

98. These fiduciary duties include candor to the court and estates about scope and remediation, and fair administration that does not confuse or impair known creditors' ability to protect their claims through clear, reliable notice.

99. Sealing/redaction orders required Kroll to safeguard and properly handle the Confidential Mailing List (names/addresses/emails) and other protected PII. The purpose of these orders was to prevent creditor targeting (e.g., phishing, impersonation).

100. Plaintiffs challenge Kroll's discretionary administration conduct (security, scoping, channel design, portal/help desk)—not any act expressly ordered by the courts—thus the claim does not seek to impose liability for judicial acts.

101. Kroll breached its fiduciary duties by failing to implement phishing-resistant privileged-access MFA and layered controls commensurate with the known sensitivity of creditor PII and Kroll's own public guidance (no SMS MFA; encryption/password protection of files at rest).

102. Kroll failed to promptly and completely disclose the scope of impacted repositories, including a months-long delay before reviewing "Unstructured Files" later found to contain DOB/driver's license data—impairing the estates' and creditors' ability to mitigate.

103. Kroll maintained email-only communications to inboxes inundated with lookalike phishing and sent Kroll/estate branded web/email points amid active impersonation and a known portal freeze, and steered victims back to Kroll websites "to verify," while omitting USPS backstops, authenticity cues, translations, strict SPF/DKIM/DMARC enforcement, and rapid lookalike takedowns.

104. By continuing to route class members through Kroll-controlled websites whose Terms purport to impose arbitration on disputes "relating to these Terms or our Site," Kroll elevated its contractual interests and exposure mitigation over the estates' interest in effective, unconfusing, rights-protective communications for known creditors.

105. Kroll failed to tailor notice to the risk environment (no USPS backstops/translation cohorts) despite discretion to do so and the availability of mailed notice consistent with sealing orders.

106. Kroll failed to escalate and document robust takedown programs and public authenticity cues in a timely way; published, independent intelligence reports documented data for sale and fake portals for months.

107. Kroll operated and/or advised unstable portals that silently toggled claim status (e.g., Verified to Unverified) and blocked tax-form submission, among other claimant workflows, without individualized explanations—frustrating creditors' ability to protect their claims.

108. Kroll's fiduciary breaches foreseeably caused estate-level disruption (freeze measures, "Cyber Issues" costs) and individual harms (phishing losses; exposure/ongoing risk; expungements/forfeitures/delays and time-value losses).

109. Plaintiffs and class members suffered non-derivative injuries: (a) out-of-pocket phishing losses; (b) exposure/loss of control of their PII; (c) mitigation/time costs; and (d) lost

distributions/time-value and expungements/forfeitures where notice was not reasonably communicated in a contaminated channel.

110. Plaintiffs seek compensatory damages, equitable relief (including disgorgement of fees attributable to the breached fiduciary functions to the extent permitted), and injunctive measures (see Count VII) to restore notice integrity at Kroll's expense (or with Kroll reimbursement) so creditor distributions are not diminished.

COUNT VI — BREACH OF IMPLIED CONTRACT

111. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

112. By collecting, holding, and using customer-creditor PII for claims administration (notice, portal verification, distribution), and by presenting official channels through which creditors must receive and act on rights-critical information, Kroll formed an implied-in-fact contract to: (i) implement reasonable security for PII and privileged access, and (ii) provide communications reasonably calculated to reach known creditors post-incident.

113. Plaintiffs and class members provided valuable PII, time, and cooperation; Kroll accepted and benefitted (through engagements and fees) while operating the communications and portal/distribution programs.

114. The implied terms arise from confidentiality orders, Kroll's court-approved roles, Kroll's published security guidance, and the official character of the case websites/portals.

115. Kroll breached its duty to protect PII by failing to implement phishing-resistant MFA and to adequately protect data at rest.

116. Kroll breached its duty to timely notify breach cohorts by delaying review of "Unstructured Files" for months, later found to contain DOB/driver's license data; failing to provide granular disclosure so class members could mitigate.

117. Kroll breached its duty to provide administrative duties by continuing noticing in an email-only in a contaminated channel, failing to deploy USPS backstops, authenticity cues, translations, sender-auth enforcement, rapid takedowns, and portal/support SLAs with individualized explanations.

118. As a direct and proximate result, Plaintiffs and class members suffered phishing/targeted attack losses, exposure/ongoing risk, mitigation/time costs, and bankruptcy process harms (expungements/forfeitures/delays and time-value losses).

119. Kroll's willful misconduct/recklessness directly and proximately caused: (i) phishing/targeted-attack losses (including the $300,000 BlockFi wallet drain), (ii) exposure and loss of control of PII with ongoing risk, (iii) mitigation/time costs, and (iv) bankruptcy-process harms (expungements/forfeitures/delays and time-value losses).

120. Plaintiffs and class members incurred out-of-pocket losses, time costs, emotional distress, and diminished value of administrative services.

121. The full scope—including the "Unstructured Files" with DOB/driver's-license data—emerged late 2023–early 2024; portal/account restrictions continued into 2025; bankruptcy-process harms matured months to a year later.

COUNT VII — DECLARATORY AND INJUNCTIVE RELIEF

122. Plaintiffs incorporate by reference herein the allegations of the previous paragraphs of this Complaint as if each were fully set forth herein in their entirety.

123. A live controversy exists over the adequacy of Kroll's post-incident communications design and the need for targeted remedial measures to ensure known creditors receive rights-critical information. Plaintiffs seek narrow, time-boxed injunctive relief that aligns with the estates' objectives and is funded by Kroll, so creditor distributions are not reduced.

124. Tailored injunctive program (time-boxed; Kroll-funded). Order Kroll to implement, for a defined period, the following:

Channel Reliability

(i) USPS First-Class Mail to defined cohorts (unverified/expunged; bounced-email; limited-English recipients; portal-locked accounts);

(ii) Bounce processing and re-send logic across channels with manual review;

Authenticity & Spoofing Control

(iii) Publication of phishing exemplars and authenticity cues on case sites (side-by-side "legitimate vs. spoof" visuals; URL patterns; known domains);

(iv) Enforcement of SPF/DKIM/DMARC alignment and 7-day takedown SLAs for lookalike domains and fake portals;

Comprehension & Access

(v) Translations of rights-critical notices for the top-10 language cohorts;

(vi) Accessible help desk with response time SLAs and individualized explanations, not boilerplate, for any claim-status change;

Portal Integrity

(vii) Audit logs for claim-status transitions; restoration paths where status changed from Verified to Unverified without claimant action;

Rights Preservation Notice

(viii) A prominent statement on each case site that viewing/using case websites or portals does not waive Security Incident claims or compel arbitration;

Governance & Reporting

(ix) Quarterly reports to the Court summarizing backstop mailings, spoof takedowns, translation coverage, and portal/desk SLAs; and

Cost Allocation

(x) Kroll shall bear (or reimburse) the reasonable costs of implementing this program so that creditor distributions are not diminished.

125. The requested relief aligns with the estates' objectives (ensuring known creditors receive rights-critical information) without burdening creditor distributions, given Kroll's role and the United States Trustee reservations in FTX.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of all of the class members, demand trial by jury on all issues triable by jury.

REQUEST FOR RELIEF

Plaintiffs, on behalf of themselves, and the Classes, request that the Court:

A. Certify the Classes, appoint Plaintiffs as class representatives, and appoint class counsel;

B. Award compensatory, consequential, and other damages in an amount to be proven at trial;

C. Enter the declaratory and injunctive relief described above, ordering that implementation costs be borne by Kroll (or reimbursed by Kroll) so that customer-creditor distributions are not diminished;

D. Award pre- and post-judgment interest as allowed by law;

E. Award attorneys' fees and costs; and

F. Grant such other and further relief as the Court deems just and proper.

Dated: November 17, 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

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 17th day of November, 2025, a true and correct copy of the foregoing document was served via the CM/ECF system, which sent notification of such filing to all counsel of record.

By: */s/Nicholas Andrew Hall*
Nicholas Andrew Hall