& IMPORTANT DISCLAIMER / AVISO IMPORTANTE

Of course. Here is the German translation of the legal disclaimer, with all original formatting and structure maintained.

***

WICHTIGER RECHTLICHER HINWEIS

Dieses Dokument wurde mit dem automatisierten Übersetzungsdienst von InstaLaw übersetzt, der von Google Gemini 2.5 Pro unterstützt wird. Diese Übersetzung wird lediglich zu Informationszwecken bereitgestellt und ist nicht als Rechtsberatung oder als Begründung eines Mandatsverhältnisses oder Anwaltsgeheimnisses zu betrachten.

HINWEIS ZUR KI-ÜBERSETZUNG:
• Diese Übersetzung wurde mithilfe von künstlicher Intelligenz (Google Gemini 2.5 Pro) erstellt.
• KI-Systeme sind anfällig für Halluzinationen und können Ungenauigkeiten oder Fehler erzeugen.
• Die Informationen werden „wie besehen“ („as-is“) ohne jegliche Gewährleistung für Richtigkeit oder Vollständigkeit bereitgestellt.
• Diese Übersetzung kann Fehler, Auslassungen oder Fehlinterpretationen enthalten.
• In rechtlichen Angelegenheiten sollten Sie immer einen qualifizierten Anwalt konsultieren und sich auf das englische Originaldokument beziehen.
• Diese Übersetzung stellt keine Rechtsberatung, keine rechtliche Vertretung dar und begründet kein Mandatsverhältnis oder Anwaltsgeheimnis.
• InstaLaw und seine verbundenen Unternehmen übernehmen keine Haftung für Fehler oder Auslassungen in dieser Übersetzung.

RECHTLICHER HINWEIS:
Das englische Originaldokument ist als alleinige maßgebliche Fassung zu betrachten. Etwaige Abweichungen, Widersprüche oder Unklarheiten zwischen dieser Übersetzung und dem englischen Originaldokument werden zugunsten der englischen Originalfassung ausgelegt. Diese Übersetzung ist nicht beglaubigt und sollte nicht für offizielle rechtliche Verfahren ohne ordnungsgemäße Überprüfung durch einen zertifizierten Übersetzer verwendet werden.

Details zur Übersetzung:
• Erstellt am: 2025-08-20T08:49:39.753Z
• Modell: Google Gemini 2.5 Pro
• Dienst: InstaLaw Translation Services

KEIN MANDATSVERHÄLTNIS:
Der Zugriff auf, das Lesen oder die Nutzung dieses übersetzten Dokuments begründet kein Mandatsverhältnis mit InstaLaw, seinen verbundenen Unternehmen oder einer anderen Partei, die mit der Übersetzung oder Verbreitung dieses Dokuments in Verbindung steht.

English Disclaimer (Original)

IMPORTANT LEGAL DISCLAIMER

This document has been translated using InstaLaw's automated translation service powered by Google Gemini 2.5 Pro. This translation is provided for convenience only and should not be considered as legal advice or as establishing any attorney-client relationship or privilege.

AI TRANSLATION NOTICE:
• This translation was generated using artificial intelligence (Google Gemini 2.5 Pro)
• AI systems are prone to hallucinations and may produce inaccuracies or errors
• The information is presented "as-is" without any warranties of accuracy or completeness
• This translation may contain errors, omissions, or misinterpretations
• For legal matters, always consult with a qualified attorney and refer to the original English document
• This translation does not constitute legal advice, legal representation, or create any attorney-client privilege or relationship
• InstaLaw and its affiliates assume no liability for any errors or omissions in this translation

LEGAL DISCLAIMER:
The original English document should be considered the sole authoritative version. Any discrepancies, conflicts, or ambiguities between this translation and the original English document shall be resolved in favor of the original English version. This translation is not certified and should not be used for official legal proceedings without proper verification by a certified translator.

TRANSLATED LEGAL DOCUMENT

IM BEZIRKSGERICHT DER VEREINIGTEN STAATEN FÜR DEN WESTLICHEN BEZIRK VON TEXAS, ABTEILUNG AUSTIN

JACOB KEVYN REPKO, einzeln und im Namen aller anderen ähnlich situierten Personen,

Kläger,

gegen

KROLL RESTRUCTURING
ADMINISTRATION LLC (vormals Prime Clerk LLC),

Beklagte.

)
) Aktenzeichen: 1:25-cv-01319
)
)
) SAMMELKLAGESCHRIFT
)
)
)
) GESCHWORENENGERICHTSVERFAHREN
) BEANTRAGT
)
)
)

SAMMELKLAGESCHRIFT

Der Kläger Jacob Kevyn Repko („Kläger“), einzeln und im Namen aller anderen ähnlich situierten Personen, macht durch den unterzeichnenden Anwalt hiermit Folgendes gegen die Beklagte Kroll Restructuring Administration LLC (vormals Prime Clerk LLC) („Kroll“ oder „Beklagte“) geltend. Basierend auf persönlichem Wissen sowie auf Information und Glauben macht der Kläger insbesondere Folgendes geltend:

ART DER KLAGE

1. Dies ist eine Sammelklage wegen einer Datenschutzverletzung und fahrlässiger Verwaltung, die sich aus dem Sicherheitsvorfall bei Kroll vom 19. August 2023 und dem anschließenden Versäumnis ergibt, gläubigerorientierte Prozesse und Mitteilungen in drei großen Krypto-Insolvenzen – FTX, BlockFi und Genesis – mit angemessener Sorgfalt zu verwalten.

2. Die Verletzung bei Kroll legte (unter anderem) Namen, Adressen, E-Mail-Adressen, Telefonnummern, Forderungskennungen/-beträge und Kopien von Forderungsnachweisformularen offen – genau die Metadaten, die Kriminelle ausnutzen, um Krypto-Opfer mit Phishing- und „Wrench“-Angriffen ins Visier zu nehmen.

3. Nach der Verletzung beharrte Kroll auf ausschließlich per E-Mail versandten kritischen Mitteilungen (einschließlich des 130. Sammelwiderspruchs von FTX, der Forderungsüberprüfung und der Fristen für Steuerformulare), obwohl (a) weit verbreitete Phishing-Imitationen viele Gläubiger dazu veranlasst hatten, das Öffnen von „Kroll“-E-Mails zu vermeiden, und (b) Kroll seine

nachgewiesene Fähigkeit, Briefe per First-Class Mail der USPS zu versenden, wenn es dies wollte, unter Beweis gestellt hatte – z. B. im Fall Genesis, wo Kroll die Benachrichtigungen über die Verletzung per First-Class Mail verschickte. 4. Bundesinsolvenzgerichte hatten die personenbezogenen Daten (pD) von Gläubigern versiegelt, um genau solche auf Krypto-Nutzer abzielenden Straftaten zu verhindern – unter Berufung auf die realen Schäden, die in der Celsius-Insolvenz zu beobachten waren (Phishing- und „Wrench"-Angriffe). Die Gerichtsakte von Genesis dokumentiert diese Bedenken in Anordnungen zur Versiegelung von Kundeninformationen. 5. Der Kläger Jacob Kevyn Repko (Dripping Springs, Texas) reichte eine Kundenforderung bei FTX ein und erhielt dann am 24. August 2023 die Benachrichtigung über die Verletzung von Kroll. Seine pD und Forderungsdaten gehörten zu den kompromittierten Daten. 6. In den folgenden Monaten funktionierte das FTX-Kundenforderungsportal (das „FTX-Portal") wiederholt fehlerhaft: Der KYC-Status des Klägers zeigte „Verifiziert" an, sprang dann zurück auf „Ausgesetzt/Unverifiziert", was ihn daran hinderte, das für den Erhalt von Ausschüttungen erforderliche IRS-Formular (W-9) hochzuladen, trotz Dutzender von Support-E-Mails. 7. Da das FTX-Portal das Hochladen von Steuerformularen von einem „verifizierten KYC"-Status abhängig macht, kann der Kläger die letzten Voraussetzungen nicht erfüllen; gemäß dem bestätigten Plan und den Mitteilungen des Trusts können Forderungen aberkannt oder Ausschüttungen verwirkt werden, wenn Steuerformulare nicht rechtzeitig hochgeladen werden. 8. Der Kläger erlitt nach der Verletzung auch einen

direkten Phishing-Verlust: Er überwies am 3. Juli 2025 um 12:43 Uhr 1,9 ETH von einem Börsenkonto in seine Hot Wallet, und diese wurden durch einen automatisierten Transaktions-Bot, der üblicherweise zum Abfangen ausstehender Überweisungen verwendet wird, an eine nicht vom Kläger kontrollierte Wallet umgeleitet, was mit Krolls eigener Warnung übereinstimmt, dass Angreifer die durchgesickerten Daten für Phishing-Angriffe auf Krypto-Konten verwenden würden. PARTEIEN 9. Der Kläger Jacob Repko ist eine natürliche Person mit Wohnsitz in Hays County, Texas. Er ist ein FTX-Kundengläubiger mit einer angemeldeten Forderung von 87.487,93 $.

10. Die Beklagte Kroll Restructuring Administration LLC ist eine LLC aus Delaware mit bedeutenden Geschäftstätigkeiten im ganzen Land, einschließlich Büros in Texas.

11. Nach Information und Glauben verklagt der Kläger auch die Unbekannten 1-5, derzeit nicht identifizierte Nicht-Kroll-Unternehmen, die, falls überhaupt, an der antragstellerorientierten Verifizierung oder der Entgegennahme von Steuerformularen beteiligt waren (einschließlich externer KYC-Anbieter). Soweit ein Nicht-Kroll-Unternehmen die KYC-Statuskennzeichnungen oder die Zugangsbeschränkung für W-9/W-8-Formulare innerhalb des FTX-Portals kontrollierte, trägt der Kläger diese Behauptungen hilfsweise vor und wird die wahren Namen ändern und ersetzen, sobald sie identifiziert sind. Sollte Kroll eine verantwortliche Drittpartei benennen, wird der Kläger diese Partei gemäß den texanischen Regeln der anteiligen Haftung rechtzeitig beiladen.

ZUSTÄNDIGKEIT UND GERICHTSSTAND

12. Dieses Gericht ist sachlich zuständig gemäß 28 U.S.C. § 1332(d) (CAFA): Die vorgeschlagenen Sammelklägergruppen umfassen mehr als 100 Mitglieder; der Gesamtstreitwert übersteigt 5.000.000 $; es besteht minimale Diversität (Kläger aus Texas gegen Beklagte aus Delaware/ New York mit Mitgliedern der Sammelklage aus dem ganzen Land/international).

13. Dieses Gericht hat die persönliche Zuständigkeit über Kroll, da Kroll Büros in Austin, Dallas und Houston unterhält, Verwaltungs-/ Benachrichtigungstätigkeiten und die Kommunikation mit Antragstellern gezielt auf Texas ausrichtet und Handlungen begangen hat, die einem Einwohner von Texas in diesem Bezirk Schaden zugefügt haben. Die Ansprüche des Klägers ergeben sich aus oder stehen im Zusammenhang mit diesem forumsbezogenen Verhalten, und die Ausübung der Zuständigkeit steht im Einklang mit den Grundsätzen eines ordnungsgemäßen Verfahrens.

14. Der Gerichtsstand ist ordnungsgemäß gemäß 28 U.S.C. § 1391(b), da ein wesentlicher Teil der Ereignisse und Schäden in diesem Bezirk stattgefunden hat: Der Kläger wohnt hier, hat hier die Mitteilungen von Kroll erhalten, hat hier das FTX-Kundenforderungsportal (claims.ftx.com) und dann Krolls elektronischen Forderungsnachweis („EPOC“) genutzt und hat hier einen Phishing-Verlust erlitten.

15. Zum jetzigen Zeitpunkt macht der Kläger keine Ansprüche gegen die Schuldner oder eine durch den Plan freigestellte Partei geltend und beantragt keine Rechtsmittel, die eine Auslegung, Änderung oder Durchsetzung des Plans oder des

Bestätigungsbeschlusses erfordern. Es handelt sich um unabhängige deliktische/ vertragliche Ansprüche gegen die Nicht-Schuldnerin Kroll. Diese Klage ist kein Kernverfahren; der Kläger beantragt ein Geschworenengerichtsverfahren und stimmt einer insolvenzrechtlichen Entscheidung nicht zu.

DEFINITIONEN

16. „FTX-Kundenforderungsportal“ oder „FTX-Portal“ bezeichnet das Portal unter claims.ftx.com, das für die Schuldner/den FTX Recovery Trust (mit Anbietern) betrieben wird, um KYC/AML und die Kontenprüfung abzuwickeln. „Kroll-Website“ bezeichnet die Website von Kroll, einschließlich der EPOC-Schnittstelle auf restructuring.ra.kroll.com, die Einreichungen des Insolvenzformulars 410 entgegennahm und das öffentliche Forderungsverzeichnis führte. Wo die Kontrolle unklar ist, trägt der Kläger hilfsweise gegen die unbekannten Beklagten vor, die ersetzt werden, sobald sie identifiziert sind.

SACHVERHALTSDARSTELLUNG

A. Krolls Verletzung betraf FTX, Genesis und BlockFi

17. Am oder um den 19. August 2023 wurde das Telefon eines Kroll-Mitarbeiters einem SIM-Swapping unterzogen, wodurch ein Angreifer auf die Cloud-Dateien von Kroll mit den Antragsdaten für jede Insolvenzmasse zugreifen konnte. Unabhängige Bedrohungsanalysen bestätigen, dass die kompromittierten Felder später von Betrugsakteuren monetarisiert und operationalisiert wurden, die auf FTX-Antragsteller und Sekundärmarkttransaktionen abzielten.

18. Krolls Einreichung im Fall Genesis gibt zu, dass die

betroffenen Daten Namen, Telefonnummern, Adressen, Forderungsnummern/-beträge, Wallet-/Coin-Guthaben und Kopien von Forderungsnachweisen umfassten.

19. Die Mitteilung von BlockFi führt weiter aus, dass Geburtsdaten, Postanschriften und Führerscheinnummern betroffen waren, und berichtet von Krolls verspäteter Identifizierung einer großen Tranche von „unstrukturierten Dateien“.

B. Gerichte versiegelten pD von Gläubigern, weil Krypto-Gläubiger einzigartigen Angriffsvektoren ausgesetzt sind

20. Im Fall Genesis erließ das Gericht Versiegelungsanordnungen zum Schutz der Namen/Kontaktdaten von Gläubigern und verwies auf die Erfahrungen im Fall Celsius, wo auf öffentliche Bekanntmachungen Phishing- und „Wrench“-Angriffe folgten.

C. Kroll wusste, dass E-Mail unsicher war, versäumte es aber, für kritische Mitteilungen den Postweg zu nutzen

21. Nach Information und Glauben warnte Kroll die Genesis-Gläubiger öffentlich vor Phishing und versandte Benachrichtigungen über die Verletzung per First-Class Mail, um die Zustellung sicherzustellen.

22. Doch im Fall FTX verließ sich Kroll bei ebenso (oder noch) folgenreichen Mitteilungen – einschließlich der Fristen des 130. Sammelwiderspruchs (z. B. KYC bis zum 1. März 2025 beginnen; bis zum 1. Juni 2025 abschließen) und der Frist für das Steuerformular – nur wenige Monate nach seiner eigenen Phishing-auslösenden Verletzung hauptsächlich auf E-Mails, obwohl es wusste, dass viele Empfänger „Kroll“-E-Mails aus Angst vor Betrug nicht öffnen oder sie in Spam-/Junk-Ordnern finden würden. Öffentliche

Bedrohungsanalysen zeigen Phishing-geführte Kontoübernahmen, bei denen die Täter die E-Mail-Adressen der Antragsteller in neue ProtonMail-Adressen änderten und schnell 2FA-Abfragen bestanden – genau der Angriff, den Krolls reiner E-Mail-Ansatz nicht gemindert hat.

23. Das FTX-Portal macht das Hochladen von W-9/W-8BEN-Formularen von der KYC-Verifizierung abhängig. Wenn das Portal einen Benutzer fälschlicherweise zurück auf „Ausgesetzt/Unverifiziert“ setzt, wird der Schritt zur Einreichung des Steuerformulars unmöglich – was das Risiko der Aberkennung der Forderung oder des Verfalls von Ausschüttungen gemäß den den Gläubigern mitgeteilten Planverfahren birgt. In einem Umfeld, in dem Antragsteller darauf trainiert sind, „Kroll“-E-Mails aufgrund aktiver Imitationen zu meiden, war ein zugangsbeschränkter, rein onlinebasierter Schritt zur Einreichung von Steuerformularen ohne eine Alternative per First-Class Mail nicht vernünftigerweise geeignet, um zu informieren oder die Durchführung zu ermöglichen.

24. Der Bestätigungsbeschluss von FTX sieht ausdrücklich vor, dass Kroll nicht für Ansprüche aus dem „Sicherheitsvorfall“ freigestellt oder entlastet wird und dass die den Kunden in einem anderen Verfahren erstattungsfähigen Schäden nicht durch Planausschüttungen begrenzt sind. Der Kläger bittet höflich um gerichtliche Kenntnisnahme dieses Auszugs aus dem Bestätigungsbeschluss gemäß Fed. R. Evid. 201.

25. Zusätzlich zur Bestellung durch das Insolvenzgericht gemäß § 156(c) für Benachrichtigungen wurde Kroll als Verwaltungsberater beauftragt, Insolvenzverwaltungsdienste gemäß seinen

Mandatsvereinbarungen und dem Bestellungsbeschluss des Gerichts zu erbringen. Diese gläubigerorientierten Aufgaben (Aufforderung/Abstimmung/ Auszählung und Bearbeitung der Kommunikation mit Antragstellern) stützen die hierin geltend gemachten

Verwaltungsverpflichtungen.

D. Die Erfahrung des Klägers

26. Der Kläger reichte seine Kundenforderung über das FTX-Portal ein und, als er dazu aufgefordert wurde, das Insolvenzformular 410 über Krolls EPOC ein.

27. Er erhielt die Benachrichtigung von Kroll über die Verletzung, die die Offenlegung seines Namens, seiner Adresse, seiner E-Mail-Adresse und seines Kontostands bestätigte und vor Phishing warnte, das auf Krypto-Vermögenswerte abzielt.

28. Nach Schwierigkeiten mit Portalsperrungen und Verzögerungen wurde der KYC-Status des Klägers am oder um den 3. November 2023 verifiziert, doch das Portal kehrte später zu „Ausgesetzt“ zurück und blockierte das Hochladen des IRS-Formulars; unzählige E-Mails an Kroll blieben unbeantwortet.

29. Nach der Verletzung wurde der Kläger Opfer von Phishing: 1,9 ETH wurden Minuten nach dem Eintreffen in seiner Hot Wallet abgezogen (Ankunft um 12:43 Uhr; Abgang um 12:49 Uhr an die Adresse des Angreifers).

30. Der Kläger hat eine angemeldete FTX-Forderung in Höhe von 87.487,93 $ und sieht sich nun dem Verlust eines Teils oder des gesamten Ausschüttungswertes gegenüber, da er aufgrund von Portalfehlfunktionen und Benachrichtigungsversäumnissen die Planvoraussetzungen nicht

erfüllen kann.

31. Der Kläger erlitt konkrete Schäden, einschließlich: (a) tatsächlicher Missbrauch – Diebstahl von 1,9 ETH innerhalb von Minuten nach Ankunft in seiner Wallet am 3. Juli 2025; (b) Zeitwert- und Ausschüttungsschäden durch blockierte Verifizierung/ Einreichung von Steuerformularen; (c) aus eigener Tasche gezahlte Minderungskosten; (d) Verlust der Privatsphäre/Kontrolle über pD; und (e) erhebliches Risiko eines zukünftigen Missbrauchs angesichts der hierin dokumentierten, auf Krypto-Nutzer abzielenden Muster.

E. Systematischer Missbrauch der durchgesickerten Antragsdaten

32. Die Vorhersehbarkeit ist keine Abstraktion: Ermittler verfolgten Betrugsfälle in Höhe von 5,6 Millionen US-Dollar, bei denen FTX-Forderungsdaten ausgenutzt wurden, einschließlich Verkäufen von Antragsdatensätzen im Dark Web und Mustern von E-Mail-Änderungen/2FA-Umgehungen – genau die Schäden, die die Gerichte durch die Versiegelung der pD von Krypto-Gläubigern verhindern wollten. Krolls gegenteilige Mitteilung, dass keine sensiblen pD gefährdet seien, führte die Verbraucher in die Irre bezüglich der Notwendigkeit, jede „Kroll“-E-Mail als verdächtig zu behandeln und eine Bestätigung per Post zu verlangen.

33. Unabhängige Bedrohungsanalysen bestätigen, dass FTX-Antragsdaten aktiv gegen Gläubiger und Gegenparteien als Waffe eingesetzt wurden. Von Juli bis November 2024 dokumentierten Ermittler Betrugsfälle in Höhe von mindestens 5,6 Millionen US-Dollar im Zusammenhang mit dem Handel von FTX-Forderungen, bei denen ein

Akteur (oder eine Gruppe) sich unter Verwendung von KI-veränderten Selfies, neuen ProtonMail-Konten und gefälschten Ausweisen als Forderungsinhaber ausgab.

34. Die Vorgehensweise des Akteurs umfasste: (a) kürzlich erstellte ProtonMail-Adressen, die die ursprüngliche E-Mail des Antragstellers ersetzten; (b) schnelle Eingabe von 2FA-Codes, was auf eine Kontoübernahme hindeutet; und (c) Geldwäsche über Einzahlungsadressen von Gate.io, CoinEx und Binance. Diese Muster sind konsistent mit einer durch Phishing geführten Kompromittierung von Anmeldedaten nach dem Kroll-Vorfall.

35. Dieselbe Untersuchung zeigt, dass FTX-Forderungsdaten auf Dark-Web-Foren beworben wurden, einschließlich Namen, Telefonnummern, E-Mails, Wallet-/Transaktionsdetails und anderer forderungsbezogener Daten – genau die Felder, deren Kompromittierung Kroll zugegeben hat (Namen, E-Mails, Telefonnummern, Postanschriften, Kontokennungen und -guthaben sowie in einigen Fällen Geburtsdaten).

36. Die Ermittler beobachteten auch E-Mail-Änderungen zu nach der Abschaltung erstellten ProtonMail-Konten für Forderungen, die ursprünglich mit anderen E-Mails eröffnet wurden, was auf eine Übernahme und Imitation von Antragstellerkonten hindeutet.

37. Der Bericht dokumentiert Blockchain-Pfade von den Wallets der Imitatoren zu CoinEx-Einzahlungsadressen und identifiziert eine zwischengeschaltete Wallet, die mit automatisierter Transaktionsaktivität in Verbindung steht; er stellt Interaktionen mit US-Börsen (Coinbase und Kraken) fest, die für KYC-Zwecke vorgeladen

werden können. Dies belegt ein zusammenhängendes, wiederholbares Betrugsmuster, das die pD von Antragstellern und Schwachstellen in den Arbeitsabläufen ausnutzt.

38. Der Bericht stellt ferner fest, dass während einer Due-Diligence-Prüfung des FTX-Portals ein „Orbeon Forms – Seite nicht gefunden“-Fehler auftrat – was mit einem fehleranfälligen Arbeitsablauf für Antragsteller und Fehlerzuständen übereinstimmt, die böswillige Akteure nachahmen können, was die Verwirrung in einem Umfeld mit hohem Phishing-Aufkommen verstärkt.

F. Falschdarstellungen und Unterlassungen nach der Verletzung

39. Kroll spielte den Umfang der Verletzung öffentlich und in der Kommunikation mit den Antragstellern herunter – und erklärte anfangs, dass keine sensiblen pD kompromittiert worden seien. In anderen von Kroll verwalteten Insolvenzen (z. B. BlockFi) gab Kroll später bekannt, dass Geburtsdaten in „unstrukturierten Daten“ enthalten waren, was seinen ursprünglichen Aussagen widersprach. Kroll teilte den FTX-Antragstellern ebenfalls mit, dass sie weiterhin mit E-Mail-basierten Arbeitsabläufen interagieren könnten, und warnte nicht davor, dass böswillige Akteure Kroll imitierten und die E-Mail-Adressen der Antragsteller in neu erstellte ProtonMail-Konten änderten, um die 2FA zu umgehen – Muster, die durch unabhängige Bedrohungsanalysen bestätigt wurden. Diese Aussagen und Unterlassungen waren wesentlich, verbraucherorientiert und irreführend, und sie verleiteten vernünftige Antragsteller dazu, das Risiko zu unterschätzen, weiterhin nur E-Mail-Kanäle zu nutzen und stärkere Abhilfemaßnahmen zu verzögern, was zu Phishing-Verlusten,

Zeitwertschäden und versäumten Fristen führte, die in aberkannten Forderungen resultierten.

SAMMELKLAGEBEHAUPTUNGEN

40. Globale Krypto-Gläubiger-Sammelklägergruppe: Alle Personen weltweit, deren pD oder Forderungsdaten, die Kroll für die Insolvenzverfahren von FTX, BlockFi oder Genesis zur Verfügung gestellt wurden, im Rahmen des Kroll-Vorfalls im August 2023 zugegriffen, exfiltriert oder einem vernünftigen Risiko ausgesetzt wurden. Die Mitgliedschaft in der Sammelklägergruppe ist aus den Benachrichtigungslisten von Kroll, den EPOC-Aufzeichnungen und den Forderungsverzeichnissen der Insolvenzen feststellbar, die Personen identifizieren, deren Daten nach Krolls Eingeständnis im Rahmen des Vorfalls zugegriffen oder einem vernünftigen Risiko ausgesetzt wurden.

41. Untergruppen der Insolvenzen: (a) FTX-Untergruppe; (b) BlockFi-Untergruppe; und (c) Genesis-Untergruppe.

Der Kläger wird bei oder vor der Zertifizierung der Sammelklage benannte Vertreter für die BlockFi- und Genesis-Untergruppen hinzufügen. 42. Untergruppen nach Schaden (über alle Insolvenzen hinweg): (i) Untergruppe für Phishing-/Krypto-Verluste; (ii) Untergruppe für Portal-/Verifizierungs-/ Steuerformularprobleme (Verlust durch Aberkennung, Zeitwertverlust und Verwaltungsschaden);
(iii) Untergruppe für Standard-Datenschutzverletzungsschäden (Verletzung der Privatsphäre, Minderungsskosten). 43. Die Kriterien der Vielzahl, Gemeinsamkeit, Typizität und Angemessenheit sind erfüllt: Gemeinsame Fragen umfassen,

ob Kroll Pflichten zur Datensicherheit, zur Angemessenheit der Benachrichtigung und zur Verwaltung des Forderungsprozesses schuldete und verletzte; ob eine reine E-Mail-Benachrichtigung nach der Verletzung angemessen war; und ob ein Unterlassungsanspruch gerechtfertigt ist.

RECHTSWAHL

44. Verhaltensregulierende Normen unterliegen dem Recht von New York (Kroll hat seinen Hauptsitz in NY und handelte von dort aus), oder hilfsweise dem Recht von Texas für Einwohner und Schäden in Texas. Die Ansprüche stehen und fallen mit den Pflichten/Handlungen, die allen Mitgliedern der Sammelklage gemeinsam sind. Fragen der Schiedsfähigkeit unterliegen dem FAA; die öffentliche Ordnung von New York verbietet die vertragliche Haftungsfreistellung für grobe Fahrlässigkeit.

KLAGEGRÜNDE

ANTRAG I

Fahrlässigkeit (Recht von New York; hilfsweise Recht von Texas)

45. Kroll schuldete dem Kläger und den Sammelklägergruppen (FTX, BlockFi und Genesis) eine Pflicht zur Anwendung angemessener Sorgfalt bei der Erhebung, Speicherung, Übermittlung und Verwaltung von pD und Forderungsdaten der Antragsteller; zur Gestaltung, zum Betrieb und zur Unterstützung eines funktionsfähigen Verifizierungs-/Steuerformular-Arbeitsablaufs; und – insbesondere nach dem Vorfall vom 19. August 2023 – zur Abgabe von Mitteilungen, die unter allen Umständen vernünftigerweise geeignet waren, die Antragsteller über rechtsbeeinflussende Fristen und

Schritte zu informieren und vorhersehbare Phishing- und Zustellbarkeitsrisiken zu mindern.

46. Diese Pflichten ergaben sich aus (a) Krolls Rollen als vom Gericht bestellter Benachrichtigungs-/Forderungsagent und Verwaltungsberater; (b) gerichtlichen Anordnungen zur Versiegelung der pD von Krypto-Gläubigern aufgrund bekannter Phishing- und physischer Sicherheitsrisiken; (c) Krolls eigenem Wissen und Warnungen, dass offengelegte E-Mail-Adressen von Antragstellern für Phishing ins Visier genommen würden; und (d) Krolls Kontrolle über die Kommunikation mit den Antragstellern und die EPOC-Aufnahme; soweit ein Nicht-Kroll-Unternehmen die KYC-Statuskennzeichnungen und die Zugangsbeschränkung für Steuerformulare innerhalb des FTX-Portals kontrollierte, trägt der Kläger diese Behauptungen hilfsweise gegen die unbekannten Beklagten vor, die ersetzt werden, sobald sie identifiziert sind. Diese Pflichten sind unabhängig von jeglichem Vertrag und nach dem Recht von New York

und Texas anerkannt, wenn das Verhalten einer Partei ein vorhersehbares Risiko von Identitäts-/Vermögensdiebstahl

für eine bekannte, begrenzte Gruppe (Krypto-Antragsteller mit versiegelten pD) schafft oder erhöht, und wenn die Entscheidungen über Benachrichtigungen und Prozesse nach einer Verletzung den Grundsätzen eines ordnungsgemäßen Verfahrens (z. B. Mullane; Jones v. Flowers) und den Datenschutz-/Benachrichtigungsanordnungen des Insolvenzgerichts unterliegen.

47. Kroll verletzte seine Pflichten unter anderem durch: (i) das Zulassen der durch SIM-Swapping ermöglichten Kompromittierung von Cloud-

Speichern mit Antragsdaten; (ii) das Versäumnis, alle betroffenen Datenspeicher unverzüglich und vollständig zu identifizieren; (iii) das Beharren – nach der Verletzung – auf reiner E-Mail-Benachrichtigung für rechtsbeeinflussende Mitteilungen, obwohl viele Antragsteller legitime Kroll-E-Mails nicht von Phishing unterscheiden konnten und obwohl Kroll die Fähigkeit und den Präzedenzfall hatte, First-Class Mail zu versenden; (iv) das Zulassen eines Ausschüttungs-Arbeitsablaufs, bei dem das Hochladen von W-9/W-8BEN blockiert war, es sei denn, der KYC-Status im FTX-Portal zeigte „Verifiziert“ an, während es versäumt wurde, einen manuellen/alternativen Einreichungsweg über Krolls EPOC oder per Post/E-Mail bereitzustellen; (v) das Versäumnis, einen manuellen/alternativen Einreichungsweg oder postalische Bestätigungen für Statusänderungen bereitzustellen; (vi) die Bereitstellung von zirkulärem, verzögertem oder unwirksamem Support, der den Schaden verlängerte und verschlimmerte; (vii) das Versäumnis, nach der Verletzung eine Härtung der Änderungskontrolle zu implementieren (postalisch versandter Code an die alte Adresse bei jeder E-Mail-/Telefonänderung; erzwungene Bedenkzeiten; manuelle Überprüfung von Änderungen zu ProtonMail-Konten, die nach November 2022 erstellt wurden), trotz Beweisen für E-Mail-Übernahmemuster gegen Antragsteller; und (viii) das Versäumnis, Dark-Web-Überwachung und Stilllegung von Nachahmer-Domains einzusetzen, die auf FTX/Kroll-Forderungsschlüsselwörter ausgerichtet waren, nachdem Angebote von Antragsdatensätzen online

beobachtet wurden. 48. Die Risiken, die Kroll schuf und nicht minderte, waren vorhersehbar: Bundesgerichte in Krypto-Fällen hatten die pD von Kunden versiegelt, um Phishing- und „Wrench“-Angriffe zu verhindern; Bundesstrafverfolgungs- und Sicherheitsrichtlinien warnen Inhaber digitaler Vermögenswerte, identifizierende Informationen privat zu halten; und Kroll selbst teilte den Antragstellern mit, dass Angreifer überzeugende E-Mails senden würden, um Konten und Wallets zu übernehmen. Unter diesen Umständen war eine reine E-Mail-Kommunikation für rechtskritische Schritte und Fristen nicht angemessen.

49. Die Handlungen und Unterlassungen von Kroll waren die unmittelbare und direkte Ursache für die Schäden des Klägers und der Mitglieder der Sammelklage. Ohne Krolls Sicherheitsversäumnisse, die reine E-Mail-Benachrichtigung, die Weigerung, für die Fristen des 130. Sammelwiderspruchs und die Frist für das Steuerformular Post zu versenden, und das fehlerhafte, zugangsbeschränkte Portal hätten der Kläger und viele Mitglieder der Sammelklage die Verifizierung rechtzeitig begonnen und abgeschlossen und Steuerformulare eingereicht; ihre Forderungen wären nicht aberkannt oder „ausgesetzt“ worden, was die Planausschüttungen verzögert hätte; und sie hätten Phishing-Verluste und Minderungsskosten vermieden.

50. Der Kläger und die Sammelklägergruppen erlitten Schäden, einschließlich, aber nicht beschränkt auf: (a) Phishing-/Krypto-Verluste (für den Kläger 1,9 ETH, die Minuten nach Erhalt abgezogen wurden); (b) Zeitwertschäden durch Ausschüttungsverzögerungen, die durch die reine E-Mail-

Benachrichtigung und die Mängel des Portals verursacht wurden; (c) Aberkennung/Verwirkung von Forderungen im Zusammenhang mit versäumten Verifizierungs-/ Steuerformularfristen; (d) aus eigener Tasche gezahlte Ausgaben (Überwachung, Härtung von Geräten/Wallets, Dokumentenbeschaffung) und verlorene Zeit; und (e) verminderte Privatsphäre und fortgesetzter Identitäts- und Vermögensdiebstahl.

51. Der Kläger und die Sammelklägergruppen fordern Ersatz von direkten Schäden und Folgeschäden in einer bei der Verhandlung nachzuweisenden Höhe, zusammen mit Verzugszinsen vor und nach dem Urteil.

ANTRAG II

Texanisches Gesetz gegen irreführende Geschäftspraktiken – Verbraucherschutzgesetz (Tex. Bus. & Com. Code § 17.41 ff.)

52. Der Kläger ist ein Verbraucher gemäß Tex. Bus. & Com. Code § 17.45(4), da er Dienstleistungen – die Kroll-Forderungsverwaltung und die gläubigerorientierten Dienstleistungen, die zum Nutzen des Klägers von den FTX-Schuldnern/dem FTX Recovery Trust erworben wurden – in Anspruch nahm und nutzte, und diese Dienstleistungen dem Kläger erbracht wurden, um ihm die Geltendmachung und den Erhalt von Ausschüttungen auf seine Forderung zu ermöglichen.

53. Kroll hat irreführende Handlungen vorgenommen, einschließlich: (1) der Darstellung, dass Dienstleistungen Eigenschaften/Vorteile hätten, die sie nicht hatten – nämlich, dass keine sensiblen pD (z. B. vollständiger Name, Postanschrift, Geburtsdatum, Wallet-/ Transaktionsdetails) entwendet wurden und dass E-Mail-Prozesse nach der Verletzung sicher seien;

(2) des Versäumnisses, zum Zeitpunkt der Transaktionen bekannte Informationen offenzulegen (dass sensible pD in „unstrukturierten Daten“ vorhanden waren; dass Imitations-/E-Mail-Änderungs-Übernahmen aktiv waren), um die Antragsteller zu veranlassen, den reinen E-Mail-Arbeitsablauf fortzusetzen; und (3) der Darstellung von Rechten/Pflichten im Rahmen des Forderungsprozesses, die sie nicht hatten – was implizierte, dass eine reine E-Mail-Benachrichtigung für rechtskritische Fristen angemessen und ausreichend sei. 54. Im Zuge eines bekannten Sicherheitsvorfalls und einer laufenden Phishing-Kampagne war das Beharren auf einer reinen E-Mail-Benachrichtigung für rechtskritische Fristen und das Unterlassen einer postalischen Absicherung und eines manuellen Einreichungskanals für Steuerformulare eine unzumutbare Vorgehensweise, die das mangelnde Wissen und die Unfähigkeit der Antragsteller, sich selbst zu schützen, in grob unfairer Weise ausnutzte. 55. Krolls DTPA-Verstöße waren der verursachende Faktor für die Schäden des Klägers, einschließlich (i) des Diebstahls von 1,9 ETH nach Phishing, (ii) Zeitwert-/Ausschüttungsschäden durch blockierte Verifizierung und Einreichung von Steuerformularen und (iii) Minderungsskosten und Verlust der Privatsphäre/Kontrolle über pD. 56. Kroll handelte wissentlich und in mancher Hinsicht vorsätzlich: Es wusste aus seinen eigenen Untersuchungen in anderen Insolvenzen (z. B. BlockFi), dass sensible pD in „unstrukturierten Daten“ existierten, teilte den Antragstellern jedoch etwas anderes mit und passte die Benachrichtigungen und Arbeitsabläufe nicht entsprechend an. 57. Der Kläger fordert

wirtschaftliche Schäden, Anwaltsgebühren, Kosten und dreifachen Schadensersatz für wissentliche/vorsätzliche Verstöße gemäß dem texanischen DTPA. 58. Der Kläger hat die vorgerichtliche Mitteilung versandt oder versendet sie gleichzeitig. Soweit eine Mitteilung aufgrund drohender Verjährung und der Notwendigkeit eines Unterlassungsanspruchs nicht möglich war, beantragt der Kläger, dass das Gericht den DTPA-Anspruch für 60 Tage ab Zustellung aussetzt, um Abhilfegespräche gemäß den gesetzlichen Bestimmungen zu ermöglichen.

ANTRAG III

New Yorker Gesetz gegen unlautere und irreführende Handlungen (hilfsweise) 59. Kroll hat sich an verbraucherorientierten irreführenden Handlungen und Praktiken beteiligt, einschließlich des Versands irreführender öffentlich zugänglicher Fallmitteilungen und Antragstellerkommunikation, des Herunterspielens der Verletzung (Angabe,

keine sensiblen pD), des Versäumnisses, wesentliche Fakten offenzulegen (pD in Dateien und in „unstrukturierten Daten“ vorhanden; aktive Imitation), und der Ermutigung zur fortgesetzten reinen E-Mail-Kommunikation in einem aktiven Phishing-Umfeld. Diese Handlungen waren in wesentlicher Weise irreführend und schädigten den Kläger. Der Kläger fordert tatsächliche Schäden, gesetzlichen Schadensersatz, angemessene Anwaltsgebühren und einen Unterlassungsanspruch gemäß New York General Business Law §§ 349(h) und 350-e.

ANTRAG IV

Grobe Fahrlässigkeit

60. Krolls Verhalten war mehr als gewöhnliche Fahrlässigkeit. Im Wissen, dass die pD von Antragstellern offengelegt worden waren, und im Wissen, dass Antragsteller aktiv von Phishing betroffen waren, beharrte Kroll bewusst auf reiner E-Mail-Kommunikation, die reich an Links und anfällig für Nachahmungen war, für rechtsbeeinflussende Fristen; weigerte sich, in großem Umfang auf den Postweg umzusteigen, obwohl es die Fähigkeit dazu hatte und den Postweg für andere kritische Mitteilungen genutzt hatte; und setzte weiterhin die Zugangsbeschränkung für die Einreichung von Steuerformularen hinter einem unzuverlässigen Forderungsportal fort, das Benutzer wiederholt ohne Erklärung zwischen „Verifiziert“ und „Ausgesetzt“ hin- und herschaltete – selbst nachdem unabhängige Informationen die fortgesetzte Imitation, E-Mail-Änderungs-Übernahmen und Geldwäschewege unter Verwendung von Antragsdaten dokumentiert hatten.

61. Krolls Versäumnis, offensichtliche Schutzmaßnahmen zu ergreifen – First-Class Mail für rechtskritische Mitteilungen, postalische Bestätigungen von Statusänderungen, einen manuellen, nicht zugangsbeschränkten Weg für Steuerformulare, Härtung der Änderungskontrolle (postalisch versandte Codes an die bestehende Adresse; Bedenkzeiten; manuelle Überprüfung von Wechseln zu kürzlich erstellten ProtonMail-Konten) und Dark-Web-Überwachung – war eine extreme Abweichung von der gewöhnlichen Sorgfalt angesichts einer hohen Wahrscheinlichkeit eines schweren Schadens für eine Bevölkerungsgruppe, deren pD genau deshalb versiegelt wurden, um Phishing und physische

Angriffe zu vermeiden.

62. Krolls grob fahrlässiges Verhalten war ein wesentlicher Faktor bei der Verursachung der Schäden des Klägers und der Sammelklägergruppen und rechtfertigt die Zuerkennung von Strafschadensersatz, um ähnliches Fehlverhalten zu bestrafen und abzuschrecken.

63. Der Kläger und die Sammelklägergruppen fordern Strafschadensersatz in einer Höhe, die ausreicht, um die Verwerflichkeit von Krolls Verhalten widerzuspiegeln und zukünftige Verstöße abzuschrecken.

ANTRAG V

Verletzung eines stillschweigenden Vertrags (Datenschutz & Forderungsverwaltung)

64. Durch die Anforderung und Annahme der pD und Forderungseinreichungen des Klägers und der Mitglieder der Sammelklage und durch die Verpflichtung, das FTX-Portal (KYC/Prüfung) und Krolls EPOC (Forderungsanmeldung) zu nutzen, um am Insolvenzforderungsverfahren teilzunehmen, schloss Kroll stillschweigende Verträge ab, um (a) diese Informationen mit angemessener Sicherheit zu schützen, (b) die Verifizierungs- und Steuerformularschritte mit angemessener Sorgfalt zu verwalten und (c) Kanäle bereitzustellen, die vernünftigerweise so gestaltet sind, dass die Antragsteller rechtsbeeinflussende Schritte abschließen können.

65. Der Kläger und die Mitglieder der Sammelklage haben ihre Leistung erbracht, indem sie genaue Informationen lieferten und den Anweisungen von Kroll folgten. Sie erwarteten vernünftigerweise, dass Kroll ihre Daten schützen und einen funktionsfähigen, sicheren

Prozess zum Abschluss der Verifizierung und zum Hochladen von Steuerformularen bereitstellen würde.

66. Kroll verletzte diese stillschweigenden Versprechen, indem es unbefugten Zugriff auf Antragsdaten zuließ; indem es in einem bekannten Phishing-Umfeld weiterhin reine E-Mail-Benachrichtigungen verwendete; indem es an einem fehlerhaften, zugangsbeschränkten Arbeitsablauf ohne alternativen Weg festhielt; und indem es versäumte, eine manuelle, nicht zugangsbeschränkte Einreichungsoption oder postalische Bestätigungen für rechtsbeeinflussende Statusänderungen bereitzustellen.

67. Als unmittelbare und direkte Folge erlitten der Kläger und die Mitglieder der Sammelklage die oben beschriebenen Schäden, einschließlich Phishing-Verlust, Zeitwert- und Ausschüttungsschäden und aus eigener Tasche gezahlter Kosten.

68. Der Kläger und die Sammelklägergruppen fordern Schadensersatz, Rückerstattung und alle anderen angemessenen Rechtsbehelfe für Krolls Verletzung des stillschweigenden Vertrags.

ANTRAG VI

Fahrlässige Übernahme einer Aufgabe (Restatement (Second) of Torts § 324A)

69. Kroll übernahm die Erbringung von Dienstleistungen, von denen es wusste, dass sie für den Schutz des Klägers und der Sammelklägergruppen notwendig waren – nämlich den Schutz der pD von Antragstellern und die Verwaltung des Verifizierungs-/ Steuerformular-Arbeitsablaufs und der rechtsbeeinflussenden Mitteilungen.

70. Kroll erbrachte diese übernommene Aufgabe fahrlässig, indem es nach der Verletzung eine reine E-Mail-

Benachrichtigung verwendete; sich weigerte, für die Fristen des 130. Sammelwiderspruchs und die Frist für das Steuerformular Post zu versenden; die Einreichung von Steuerformularen hinter einem unzuverlässigen, statusabhängigen Arbeitsablauf beschränkte; und versäumte, einen alternativen Weg oder postalische Bestätigungen bereitzustellen.

71. Krolls fahrlässige Leistung erhöhte das Schadensrisiko für den Kläger und die Mitglieder der Sammelklage (verpasste oder ignorierte Mitteilungen, Sperrungen durch Statuswechsel, Phishing) und war ein wesentlicher Faktor für die daraus resultierenden Verluste.

72. Der Kläger und viele Mitglieder der Sammelklage verließen sich auf die Übernahme durch Kroll – sie nutzten das FTX-Portal und die Antragstellerkommunikation/ EPOC von Kroll wie angewiesen und verzichteten auf andere Schritte, da Kroll der ausschließliche Kanal für die Verifizierung und Forderungsverwaltung war.

73. Der Kläger und die Sammelklägergruppen haben Anspruch auf Schadensersatz, der unmittelbar durch Krolls fahrlässige Übernahme einer Aufgabe verursacht wurde.

ANTRAG VII

Fahrlässige Benachrichtigung und Forderungsbearbeitung nach der Verletzung

74. Nach dem Vorfall vom 19. August 2023 hatte Kroll eine erhöhte Pflicht, vorhersehbare Schäden zu mindern und Benachrichtigungen und Prozessanpassungen bereitzustellen, die vernünftigerweise geeignet waren, die Antragsteller zu erreichen und eine rechtzeitige Einhaltung rechtsbeeinflussender Schritte zu ermöglichen.

75. Kroll verletzte diese Pflicht, indem es sich weiterhin auf reine E-Mail-Benachrichtigungen verließ – trotz weit verbreitetem Phishing und Spam-Filterung, die auf Kroll-ähnliche E-Mails abzielten – und indem es versäumte, für die folgenreichsten Mitteilungen auf den Postweg umzusteigen, einschließlich der Fristen des 130. Sammelwiderspruchs von FTX

(Beginn bis 1. März 2025 und Abschluss bis 1. Juni 2025) und der Frist für das Steuerformular.

Der bestätigte Plan enthielt keine festen Daten im Plantext; daher machte Krolls Wahl des Kanals diese Mitteilungen ergebnisbestimmend. Viele vernünftige Antragsteller öffneten Kroll-E-Mails nicht, weil dies während aktiver Phishing-Kampagnen wie „Russisches Roulette“ erschien; viele Mitteilungen landeten in Junk-/Spam-Ordnern und blieben ungelesen. 76. Unabhängig davon betrieb FTX ein Portal, das die Einreichung von W-9/W-8BEN blockierte, es sei denn, der Status war „KYC Verifiziert“, doch das System setzte verifizierte Benutzer fälschlicherweise zurück auf „Ausgesetzt/Unverifiziert“, ohne manuelle Übersteuerung, ohne postalische Bestätigung von Statusänderungen und ohne alternativen Einreichungsweg – was eine vermeidbare Nichteinhaltung garantierte. 77. Krolls Support-Kommunikation verschlimmerte diese Versäumnisse – sie gab standardisierte „versuchen Sie es erneut“- und „behoben“-Nachrichten aus, leitete Antragsteller an andere Posteingänge weiter und bot keine dauerhafte Lösung – während die Fristen für die Aberkennung und das Steuerformular näher rückten. 78. Kroll stellte fälschlicherweise dar, dass keine sensiblen pD betroffen seien, und räumte später

in einer anderen Krypto-Insolvenz (BlockFi) das Vorhandensein von Geburtsdaten in „unstrukturierten Daten“ ein, wodurch die Wachsamkeit verringert und der Erfolg von Phishing erhöht wurde. 79. Als unmittelbare und direkte Folge von Krolls fahrlässiger Benachrichtigung und Forderungsbearbeitung verpassten der Kläger und die Mitglieder der Sammelklage die Verifizierungs- und Steuerformularanforderungen oder konnten sie nicht erfüllen, die sie sonst erfüllt hätten, erlitten Phishing-Verluste und erlitten Zeitwert- und Verwaltungsschäden. 80. Der Kläger und die Sammelklägergruppen fordern Schadensersatz für diese Verletzungen und eine Feststellung, dass Krolls Benachrichtigungs-/ Bearbeitungspraktiken nach der Verletzung unter den gegebenen Umständen unangemessen und rechtswidrig waren. 81. Der Kläger und die Sammelklägergruppen beantragen ferner eine Unterlassungsanordnung, die eine mehrkanalige Benachrichtigung (E-Mail und First-Class Mail mit getippten URLs/eindeutigen Codes), postalische Bestätigungen für jede rechtsbeeinflussende Statusänderung, definierte Abhilfefristen vor der Aberkennung und einen manuellen/alternativen Kanal für die Verifizierung und die Einreichung von Steuerformularen vorschreibt. Kroll verwaltet weiterhin die gläubigerorientierte

Kommunikation und die Aufzeichnungen in Bezug auf diese Insolvenzen, sodass das Risiko zukünftiger Schäden ohne gerichtlich angeordnete Schutzmaßnahmen fortbesteht.

ANTRAG VIII

Fahrlässige Falschdarstellung (Aussagen zum Prozess nach der Verletzung)

82. Kroll stellte in der Kommunikation nach der Verletzung dar, dass Verifizierungsfehler „behoben“ seien, dass Antragsteller es „erneut versuchen“ sollten oder dass der Status „Verifiziert“ sei, obwohl das System weiterhin auf „Ausgesetzt/Unverifiziert“ zurückfiel und die Einreichung von Steuerformularen blockierte. Krolls Rolle als vom Gericht bestellter Forderungs-/ Benachrichtigungsagent und Verwaltungsberater versetzte es in eine Position des einzigartigen und vertrauenswürdigen Zugangs zu Gläubigerinformationen und der Prozesskontrolle, was eine besondere Beziehung schuf, die ausreicht, um eine Haftung für fahrlässige Falschdarstellung zu begründen.

83. Kroll lieferte diese Informationen im Rahmen seiner professionellen Verwaltungspflichten und wandte dabei keine angemessene Sorgfalt an. Der Kläger und die Mitglieder der Sammelklage verließen sich berechtigterweise darauf, indem sie mit demselben fehlerhaften Arbeitsablauf fortfuhren und auf Eskalationsalternativen verzichteten, was zu versäumten Fristen, Zeitwertverlusten und Aberkennung führte.

84. Der Kläger fordert Schadensersatz, der unmittelbar durch dieses Vertrauen verursacht wurde.

ANTRAG IX
Ungerechtfertigte Bereicherung (hilfsweise)

85. Kroll erhielt eine erhebliche Vergütung für seine Tätigkeit als Benachrichtigungs-/ Forderungsagent und Verwaltungsberater in den Krypto-Insolvenzen, während es die Kosten und Risiken seiner mangelhaften Sicherheit und Verwaltung nach der Verletzung auf die Antragsteller abwälzte.

86. Es wäre unbillig, wenn Kroll diese Vorteile behalten würde, ohne die von ihm verursachten Verluste zu erstatten und ohne Abhilfemaßnahmen zu finanzieren (einschließlich Überwachung, Sicherheitsverbesserungen, erneute Benachrichtigung und wieder geöffnete Einreichungsfenster).

87. Der Kläger macht ungerechtfertigte Bereicherung hilfsweise zu seinen Vertrags- und Deliktsansprüchen geltend, falls das Gericht feststellt, dass kein durchsetzbarer Vertrag Krolls Pflichten gegenüber den Antragstellern regelt.

88. Der Kläger und die Sammelklägergruppen fordern Rückerstattung und Herausgabe unrechtmäßig erlangter Vorteile sowie Gebührenverrechnungen, die den verursachten Schäden entsprechen.

ANTRAG X

Feststellungs- und Unterlassungsanspruch (28 U.S.C. §§ 2201-02)

89. Es besteht eine tatsächliche, justiziable Streitigkeit bezüglich Krolls fortlaufender Verpflichtungen, die Daten der Antragsteller zu sichern, eine angemessene Benachrichtigung über rechtsbeeinflussende Schritte zu geben und einen funktionsfähigen Verifizierungs-/ Steuerformularprozess zu betreiben, der konforme Antragsteller nicht willkürlich blockiert.

90. Der Kläger beantragt eine Feststellung, dass Krolls reine E-Mail-Benachrichtigung und das zugangsbeschränkte Portal nach der Verletzung unter den gegebenen Umständen unangemessen waren und dass Kroll künftig Prozesse anwenden muss, die vernünftigerweise geeignet sind, die Antragsteller zu erreichen und zu schützen.

91. Der Kläger beantragt

auch eine dauerhafte Unterlassungsanordnung, die Kroll für nicht weniger als drei (3) Jahre verpflichtet, Folgendes umzusetzen: (a) mehrkanalige Benachrichtigung (E-Mail und First-Class Mail) für jede rechtsbeeinflussende Frist, mit getippten URLs/eindeutigen Zugangscodes und ohne anklickbare Links; (b) postalische Bestätigungen jeder Verifizierungsstatusänderung und eine Mindest-Abhilfefrist von 30 Tagen vor Aberkennung oder Verfall; (c) Härtung der Änderungskontrolle: postalisch versandte Einmalcodes an die bestehende Postanschrift, bevor eine E-Mail-/Telefonänderung wirksam wird; (d) eine 14-tägige Bedenkzeit für Änderungen der Kontaktmethode, es sei denn, sie werden durch einen postalisch versandten Code verifiziert; (e) manuelle Überprüfung von Wechseln zu kürzlich erstellten ProtonMail- oder anderen Hochrisiko-Domains; (f) eine manuelle/alternative Methode zur Durchführung der Verifizierung und zur Einreichung von W-9/ W-8BEN, die nicht durch Portal-Flags beschränkt ist, mit einem veröffentlichten Eskalations-SLA (5 Werktage Eskalation; 10 Werktage Lösung); (g) unveränderliche Prüfprotokolle von Statusänderungen und eine manuelle Übersteuerungsmöglichkeit; (h) branchenübliche Zustellbarkeits- und Anti-Spoofing-Kontrollen (dedizierte Domains, DMARC/SPF/DKIM-Durchsetzung, Link-Tracking-Disziplin, Stilllegung von Nachahmer-Domains, die auf FTX/Kroll/ Forderungsschlüsselwörter ausgerichtet sind); (i) unabhängige jährliche Prüfungen der Sicherheit, Zustellbarkeit und des Portal-Arbeitsablaufs mit Berichten, die dem Gericht zur Verfügung stehen; und (j)

finanzierte Kredit-/ID- und Krypto-Kontoüberwachung sowie ein Programm zur Erstattung von Phishing-Verlusten für betroffene Antragsteller. 92. Die beantragte Abhilfe wird zukünftige Schäden verhindern, die durch Schadensersatz allein nicht behoben werden können, einen fairen Zugang zu Ausschüttungen gewährleisten und Krolls Praktiken an die vorhersehbaren Risiken anpassen, die für Krypto-Gläubiger einzigartig sind. 93. Dem Kläger und den Sammelklägergruppen fehlt ein angemessener Rechtsbehelf für die zukünftigen Schäden, die durch die beantragten Unterlassungsanordnungen angegangen werden; eine finanzielle Entschädigung kann eine rechtzeitige, sichere und effektive Verwaltung der laufenden Verpflichtungen der Antragsteller nicht gewährleisten. 94. Die Abwägung der Billigkeitsinteressen und das öffentliche Interesse sprechen für eine Unterlassungsanordnung, da sie die Rechte Tausender von Antragstellern schützt, gehört zu werden und Ausschüttungen ohne unangemessenes Risiko von Betrug oder Aberkennung aufgrund fehlerhafter Prozesse zu erhalten. 95. Der Kläger und die Sammelklägergruppen fordern auch ihre angemessenen Anwaltsgebühren und Kosten, soweit gesetzlich zulässig, einschließlich unter den Common-Fund-/Common-Benefit-Doktrinen und den Billigkeitsbefugnissen des Gerichts.

SCHIEDSVEREINBARUNG/ SAMMELKLAGEVERZICHT 96. Das FTX-Portal ist nicht Krolls „Website“, wie in Krolls Nutzungsbedingungen definiert. Der Kläger hat im FTX-Portal keinen Kroll-Bedingungen zugestimmt. Das FTX-Portal enthielt nur eine FTX-Einwilligung zur Datenverarbeitung; es zeigte keine Kroll-Bedingungen, keine

Schiedsvereinbarung und keinen Sammelklageverzicht an. Soweit Kroll auf eine separate Click-Through-Vereinbarung auf seiner EPOC- oder Kroll-Website verweist, ist die Klausel eng und fakultativ und gilt nur für Streitigkeiten, „die sich aus oder im Zusammenhang mit diesen Bedingungen oder unserer Website ergeben“, und es gibt keine Delegationsklausel – daher entscheidet dieses Gericht über die Schiedsfähigkeit. Die Ansprüche des Klägers ergeben sich aus Krolls vom Gericht bestellten Verwaltungs- und Datensicherheitspflichten (M365-Verletzung; Benachrichtigungskanäle nach der Verletzung; Fehlen eines nicht zugangsbeschränkten Weges für Steuerformulare), die unabhängig von jeglicher Website-Nutzung bestehen und außerhalb jeder auf die Website beschränkten Klausel fallen. Alternativ ist die Erzwingung einer Schiedsvereinbarung/eines Sammelklageverzichts als Bedingung für die Einreichung eines Bundesformulars 410 verfahrensrechtlich sittenwidrig; und nach der öffentlichen Ordnung von New York kann grobe Fahrlässigkeit nicht vertraglich entschuldigt werden. Die Formulierung „auf individueller Basis“ in den Bedingungen ist auf das Schiedsverfahren beschränkt; es gibt keinen eigenständigen Verzicht auf Sammelklagen vor Gericht. Die Ausnahme für den Kroll-Sicherheitsvorfall im Plan bestätigt, dass es sich um unabhängige Deliktsansprüche Dritter handelt, die voraussichtlich ‚in einem anderen Verfahren‘ fortgesetzt werden, was jede Theorie der Nichtunterzeichnung untergräbt.

ANTRAG AUF RECHTSSCHUTZ

DAHER beantragt der Kläger, einzeln und im Namen der anderen Mitglieder der in dieser Klageschrift vorgeschlagenen

Sammelklägergruppen, höflich, dass das Gericht ein Urteil zu ihren Gunsten und gegen die Beklagte erlässt, wie folgt:

A. Für einen Beschluss, der diese Klage als Sammelklage zulässt und den Kläger und seinen Anwalt zur Vertretung der Sammelklägergruppen bestellt;

B. Für eine billigkeitsrechtliche Anordnung, die die Rückerstattung und Herausgabe der Einnahmen vorschreibt, die aufgrund des rechtswidrigen Verhaltens der Beklagten unrechtmäßig einbehalten wurden;

C. Für die Zuerkennung von tatsächlichen Schäden, Schadensersatz, gesetzlichem Schadensersatz und gesetzlichen Strafen in einer zu bestimmenden Höhe, wie gesetzlich zulässig;

D. Für die Zuerkennung von Strafschadensersatz, wie gesetzlich zulässig;

E. Rechtsbehelfe nach dem texanischen DTPA: wirtschaftliche Schäden, dreifacher Schadensersatz für wissentliche/ vorsätzliche Verstöße und angemessene und notwendige Anwaltsgebühren (DTPA § 17.50(d));

F. New York GBL §§ 349/350 (hilfsweise): gesetzlicher Schadensersatz und Anwaltsgebühren;

G. Für die Zuerkennung von Anwaltsgebühren und Kosten sowie sonstigen Auslagen, einschließlich Sachverständigenhonoraren;

H. Verzugszinsen vor und nach dem Urteil auf alle zugesprochenen Beträge; und

I. Solche weiteren und zusätzlichen Rechtsbehelfe, die dieses Gericht für gerecht und angemessen hält.

Datum: 19. August 2025

Hochachtungsvoll eingereicht,

HALL ATTORNEYS, P.C.
Von: /s/ Nicholas Andrew Hall
Nicholas Andrew Hall
Anwaltskammer-Nr. 24069863
nhall@hallattorneys.com

P.O. Box 1370
Edna, Texas 77957
+1 713 428 8967

ANWALT DES KLÄGERS
UND DER
MUTMASSLICHEN SAMM
ELKLÄGERGRUPPEN