
TRANSLATED DOCUMENT

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

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

Kläger,

gegen

KROLL RESTRUCTURING
ADMINISTRATION LLC (v/k/a Prime Clerk LLC),

Beklagte.

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

SAMMELKLAGESCHRIFT

Der Kläger Jacob Kevyn Repko („Kläger“), im eigenen Namen und im Namen aller anderen ähnlich situierten Personen, trägt durch den unterzeichnenden Anwalt hiermit Folgendes gegen die Beklagte Kroll Restructuring Administration LLC (v/k/a Prime Clerk LLC) („Kroll“ oder „Beklagte“) vor. Basierend auf persönlicher Kenntnis sowie auf Informationen und Überzeugung trägt der Kläger insbesondere Folgendes vor:

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, die an Gläubiger gerichteten Prozesse und Mitteilungen in drei großen Krypto-Insolvenzverfahren – FTX, BlockFi und Genesis – mit angemessener Sorgfalt zu verwalten.

2. Die Verletzung bei Kroll legte (neben anderen Feldern) 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. Omnibus-Einspruchs von FTX, der Forderungsüberprüfung und der Fristen für Steuerformulare), obwohl (a) weit verbreitete Phishing-Imitationen viele Gläubiger darauf trainiert hatten, das Öffnen von „Kroll"-E-Mails zu vermeiden, und (b) Kroll seine nachgewiesene Fähigkeit demonstriert hatte, Briefe per First-Class Mail der USPS zu versenden, wenn es dies wollte – z. B. im Fall Genesis, wo Kroll die Benachrichtigungen über die Verletzung per First Class Mail verschickte.

4. Bundesinsolvenzgerichte hatten die PII (personenbezogenen Daten) von Gläubigern versiegelt, um gezielte Verbrechen gegen Krypto-Inhaber zu verhindern – unter Berufung auf die realen Schäden, die im Celsius-Insolvenzverfahren zu beobachten waren (Phishing- und „Wrench"-Angriffe). Die Gerichtsakte im Fall Genesis dokumentiert diese Bedenken in Anordnungen zur Versiegelung von Kundeninformationen.

5. Der Kläger Jacob Kevyn Repko (Dripping Springs, Texas) meldete eine Kundenforderung bei FTX an und erhielt daraufhin am 24. August 2023 die Benachrichtigung von Kroll über die Datenschutzverletzung. Seine PII 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 aber wieder auf „Ausgesetzt/Unverifiziert" zurück, was ihn daran hinderte, das für den Erhalt von Ausschüttungen erforderliche IRS-Formular (W-9) hochzuladen, trotz Dutzender Support-E-Mails.

7. Da das FTX-Portal das Hochladen von Steuerformularen von einem „verifizierten KYC" abhängig macht, kann der Kläger die letzten Voraussetzungen nicht erfüllen; gemäß dem bestätigten Plan und den Mitteilungen des Trusts können Forderungen gestrichen oder Ausschüttungen verwirkt werden, wenn Steuerformulare nicht fristgerecht hochgeladen werden.

8. Der Kläger erlitt nach der Datenschutzverletzung auch einen direkten Phishing-Verlust: Er überwies am 3. Juli 2025 um 12:43 Uhr 1,9 ETH von einem Börsenkonto auf seine Hot Wallet, und diese wurden durch einen automatisierten Transaktionsbot, der üblicherweise zum Abfangen ausstehender Überweisungen verwendet wird, auf 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 nach dem Recht von Delaware mit bedeutenden Geschäftstätigkeiten im ganzen Land, einschließlich Büros in Texas.

11. Nach bestem Wissen und Gewissen verklagt der Kläger auch die Unbekannten 1-5, derzeit nicht identifizierte Nicht-Kroll-Unternehmen, die, falls überhaupt, an der an Antragsteller gerichteten Verifizierung oder der Entgegennahme von Steuerformularen beteiligt waren (einschließlich externer KYC-Anbieter). Soweit ein Nicht-Kroll-Unternehmen die KYC-Statuskennzeichnungen oder die Abhängigkeit des W-9/W-8-Uploads im FTX-Portal kontrollierte, macht der Kläger diese Vorwürfe hilfsweise geltend und wird die wahren Namen nach deren Identifizierung ändern und ersetzen. Sollte Kroll eine verantwortliche Drittpartei benennen, wird der Kläger diese Partei gemäß den texanischen Regeln zur 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 eine minimale Diversität (Kläger aus Texas gegen Beklagte aus Delaware/New York mit Mitgliedern der Sammelklägergruppe aus dem ganzen Land/international).

13. Dieses Gericht hat die persönliche Zuständigkeit über Kroll, da Kroll Büros in Austin, Dallas und

Houston unterhält, Verwaltungs-/Benachrichtigungsarbeiten und die Kommunikation mit Antragstellern gezielt nach Texas lenkt 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 Gerichtsbarkeit steht im Einklang mit dem Gebot eines fairen Verfahrens (due process).

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

15. Derzeit macht der Kläger keine Ansprüche gegen die Schuldner oder eine durch den Plan freigestellte Partei geltend und beantragt keine Abhilfe, die eine Auslegung, Änderung oder Durchsetzung des Plans oder der Bestätigungsanordnung erfordern würde. Es handelt sich um unabhängige Delikts-/Vertragsansprüche gegen die Nicht-Schuldnerin Kroll. Diese Klage ist kein Kernverfahren; der Kläger beantragt ein Schwurgerichtsverfahren 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 Kontoprüfung 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 Forderungsregister führte. Wo die Kontrolle unklar ist, klagt der Kläger hilfsweise gegen unbekannte Beklagte, die nach Identifizierung ersetzt werden sollen.

SACHVERHALTSDARSTELLUNG

A. Krolls Datenschutzverletzung betraf FTX, Genesis und BlockFi

17. Am oder um den 19. August 2023 unterzog ein Angreifer das Telefon eines Kroll-Mitarbeiters einem SIM-Swapping und verschaffte sich so Zugriff auf Krolls Cloud-Dateien mit Antragsstellerdaten für jede Insolvenzmasse. Unabhängige Threat-Intelligence-Berichte bestätigen, dass die kompromittierten Felder später von Betrügern monetarisiert und operationalisiert wurden, die FTX-Antragsteller und Sekundärmarkttransaktionen ins Visier nahmen.

18. Krolls Einreichung im Fall Genesis räumt ein, dass zu den betroffenen Daten Namen, Telefonnummern, Adressen, Forderungsnummern/-beträge, Wallet-/Coin-Guthaben und Kopien von Forderungsnachweisen gehörten.

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

B. Gerichte versiegelten die PII von Gläubigern, da 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-Mails unsicher waren, versäumte es aber, für kritische Mitteilungen den Postweg zu nutzen

21. Nach bestem Wissen und Gewissen warnte Kroll die Genesis-Gläubiger öffentlich vor Phishing und versandte Benachrichtigungen über die Datenschutzverletzung per First-Class Mail, um die Zustellung sicherzustellen.

22. Dennoch verließ sich Kroll im Fall FTX bei ebenso (oder noch) wichtigeren Mitteilungen – einschließlich der Fristen für den 130. Omnibus-Einspruch (z. B. Beginn des KYC bis 1. März 2025; Abschluss bis 1. Juni 2025) und der Frist für das Steuerformular – nur Monate nach seiner eigenen, Phishing auslösenden Datenschutzverletzung hauptsächlich auf E-Mails, obwohl Kroll wusste, dass viele Empfänger „Kroll“-E-Mails aus Angst vor Betrug nicht öffnen oder sie in Spam-/Junk-Ordnern finden würden. Öffentliche Threat-Intelligence-Berichte zeigen durch Phishing verursachte Kontoübernahmen, bei denen die Täter die E-Mail-Adressen der Antragsteller in neue ProtonMail-Adressen änderten und schnell 2FA-Herausforderungen bestanden – genau der Angriff, den Krolls reiner E-Mail-Ansatz ungemindert ließ.

23. Das FTX-Portal macht das Hochladen von W-9/W-8BEN von der KYC-Verifizierung abhängig. Wenn das Portal einen Benutzer fälschlicherweise auf „Ausgesetzt/Unverifiziert“ zurücksetzt, wird der Schritt des Steuerformulars unmöglich – was das Risiko der Streichung 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 abhängiger, rein onlinebasierter Schritt für das Steuerformular ohne eine Alternative per First-Class Mail nicht vernünftigerweise dazu geeignet, über den Abschluss zu informieren oder ihn zu ermöglichen.

24. Die Bestätigungsanordnung im Fall FTX sieht ausdrücklich vor, dass Kroll nicht für Ansprüche aus dem „Sicherheitsvorfall“ freigestellt oder entschuldet wird und dass der von Kunden in einem anderen Verfahren erstattungsfähige Schaden nicht durch Planausschüttungen begrenzt ist. Der Kläger beantragt respektvoll die gerichtliche Kenntnisnahme dieses Auszugs aus der Bestätigungsanordnung gemäß Fed. R. Evid. 201.

25. Zusätzlich zur Beauftragung durch das Insolvenzgericht gemäß § 156(c) für Benachrichtigungen wurde Kroll als administrativer Berater beauftragt, Insolvenzverwaltungsdienste gemäß seinen Auftragsunterlagen und der Beauftragungsanordnung des Gerichts zu erbringen. Diese an die Gläubiger gerichteten Pflichten (Aufforderung/Abstimmung/Auszählung und Bearbeitung der Gläubigerkommunikation) stützen die hierin geltend gemachten Verwaltungspflichten.

D. Die Erfahrung des Klägers

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

27. Er erhielt die Benachrichtigung von Kroll über die Datenschutzverletzung, 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. Nachdem er mit Portalsperrungen und Verzögerungen zu kämpfen hatte, wurde der KYC-Status des Klägers am oder um den 3. November 2023 verifiziert, doch das Portal kehrte später zu „Ausgesetzt“ zurück, was das Hochladen des IRS-Formulars blockierte; unzählige E-Mails an Kroll blieben unbeantwortet.

29. Nach der Datenschutzverletzung 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, darunter: (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) Auslagen für Schadensminderungsmaßnahmen; (d) Verlust der Privatsphäre/Kontrolle über PII; und (e) ein erhebliches Risiko zukünftigen Missbrauchs angesichts der hierin dokumentierten, auf Krypto abzielenden Muster.

E. Systematischer Missbrauch durchgesickerter Antragsstellerdaten

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

33. Unabhängige Threat-Intelligence-Berichte bestätigen, dass FTX-Antragsstellerdaten 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 stehen im Einklang mit einer durch Phishing verursachten Kompromittierung von Anmeldeinformationen nach dem Kroll-Vorfall.

35. Dieselbe Untersuchung zeigt, dass FTX-Forderungsdaten in Darknet-Foren beworben wurden, einschließlich Namen, Telefonnummern, E-Mails, Wallet-/Transaktionsdetails und anderer forderungsbezogener Daten – genau die Felder, deren Kompromittierung Kroll eingeräumt hatte (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 Antragsstellerkonten 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 PII von Antragstellern und Schwachstellen im Arbeitsablauf ausnutzt.

38. Der Bericht stellt ferner fest, dass während einer Due-Diligence-Prüfung des FTX-Portals ein Fehler „Orbeon Forms – Page Not Found“ auftrat – was mit einem fragilen 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 Datenschutzverletzung

39. Kroll spielte öffentlich und in der Kommunikation mit Antragstellern das Ausmaß der Datenschutzverletzung herunter – und erklärte anfangs, dass keine sensiblen PII kompromittiert worden seien. In anderen von Kroll verwalteten Insolvenzmassen (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 2FA zu umgehen – Muster, die durch unabhängige Threat-Intelligence 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 der Streichung von Forderungen resultierten.

SAMMELKLAGEVORWÜRFE

40. Globale Krypto-Gläubiger-Sammelklägergruppe: Alle Personen weltweit, deren PII oder Forderungsdaten, die Kroll für die Insolvenzverfahren von FTX, BlockFi oder Genesis zur Verfügung gestellt wurden, beim Kroll-Vorfall im August 2023 abgerufen, exfiltriert oder einem angemessenen Risiko ausgesetzt waren. Die Mitgliedschaft in der Sammelklägergruppe ist aus Krolls Benachrichtigungslisten, EPOC-Aufzeichnungen und den Forderungsregistern der Insolvenzmassen feststellbar, die Personen identifizieren, deren Daten nach Krolls Eingeständnis bei dem Vorfall abgerufen oder einem angemessenen Risiko ausgesetzt waren.

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

Der Kläger wird bei oder vor der Zertifizierung der Sammelklage benannte Vertreter für die Untergruppen BlockFi und Genesis hinzufügen.

42. Untergruppen nach Schaden (über alle Insolvenzmassen hinweg): (i) Untergruppe Phishing/Krypto-Verlust; (ii) Untergruppe Portal/Verifizierung/Steuerformular (Verlust durch Streichung, Zeitwertverlust und administrativer Schaden); (iii) Untergruppe für Standard-Datenschutzverletzungsschäden (Verletzung der Privatsphäre, Minderungsskosten).

43. Mitgliederzahl, Gemeinsamkeit, Typizität und Angemessenheit sind erfüllt: Zu den gemeinsamen Fragen gehören, ob Kroll Pflichten zur Datensicherheit, zur Angemessenheit von Mitteilungen und zur Verwaltung des Forderungsprozesses schuldete und verletzte; ob eine reine E-Mail-Benachrichtigung nach der Datenschutzverletzung angemessen war; und ob ein Unterlassungsanspruch gerechtfertigt ist.

RECHTSWAHL

44. Die verhaltensregulierenden Standards unterliegen dem Recht von New York (Kroll hat seinen Hauptsitz in NY und handelte von dort aus), oder alternativ dem Recht von Texas für Einwohner und Schäden in Texas. Die Ansprüche stehen und fallen mit Pflichten/Handlungen, die allen Mitgliedern der Sammelklägergruppe gemeinsam sind. Fragen der Schiedsfähigkeit unterliegen dem FAA; die öffentliche Ordnung von New York verbietet die vertragliche Entlastung von grober Fahrlässigkeit.

KLAGEGRÜNDE

KLAGEGRUND I

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

45. Kroll schuldete dem Kläger und den Sammelklägergruppen (FTX, BlockFi und Genesis) die Pflicht, bei der Erhebung, Speicherung, Übermittlung und Verwaltung der PII und Forderungsdaten von Antragstellern angemessene Sorgfalt walten zu lassen; einen funktionalen Arbeitsablauf für die Verifizierung/das Steuerformular zu entwerfen, zu betreiben und zu unterstützen; und – insbesondere nach dem Vorfall vom 19. August 2023 – Mitteilungen zu machen, die unter allen Umständen vernünftigerweise geeignet sind, 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 administrativer Berater; (b) gerichtlichen Anordnungen zur Versiegelung der PII von Krypto-Gläubigern aufgrund bekannter Phishing- und physischer Sicherheitsrisiken; (c) Krolls eigenem Wissen und Warnungen, dass offengelegte E-Mail-Adressen von Antragstellern für Phishing-Angriffe ins Visier genommen würden; und (d) Krolls Kontrolle über die Kommunikation mit Antragstellern und die EPOC-Annahme; soweit ein Nicht-Kroll-Unternehmen die KYC-Statuskennzeichnungen und die Abhängigkeit des Steuerformular-Uploads im FTX-Portal kontrollierte, macht der Kläger diese Vorwürfe hilfsweise gegen unbekannte Beklagte geltend, die nach Identifizierung ersetzt werden sollen. 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 des Identitäts-/Vermögensdiebstahls für eine bekannte, begrenzte Gruppe (Krypto-Antragsteller mit versiegelten PII) schafft oder erhöht, und wenn die Entscheidungen über Benachrichtigung und Verfahren nach einer Datenschutzverletzung den Grundsätzen eines fairen Verfahrens (z. B. Mullane; Jones v. Flowers) und den Datenschutz-/Benachrichtigungsanordnungen des Insolvenzgerichts unterliegen.

47. Kroll verletzte seine Pflichten unter anderem dadurch, dass es: (i) die durch SIM-Swapping ermöglichte Kompromittierung von Cloud-Speichern mit Antragsstellerdaten zuließ; (ii) es versäumte, alle betroffenen Datenspeicher unverzüglich und vollständig zu identifizieren; (iii) es – nach der Datenschutzverletzung – bei der reinen E-Mail-Benachrichtigung für rechtsbeeinflussende Mitteilungen beharrte, obwohl viele Antragsteller legitime Kroll-E-Mails nicht von Phishing unterscheiden konnten und obwohl Kroll die Fähigkeit und den Präzedenzfall hatte, per First-Class Mail zu versenden; (iv) es einen Ausschüttungsworkflow zuließ, 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 versäumte, einen manuellen/alternativen Einreichungsweg über Krolls EPOC oder per Post/E-Mail bereitzustellen; (v) es versäumte, einen manuellen/alternativen Einreichungsweg oder postalische Bestätigungen für Statusänderungen bereitzustellen; (vi) es zirkulären, verzögerten oder unwirksamen Support leistete, der den Schaden verlängerte und verschlimmerte; (vii) es versäumte, nach der Datenschutzverletzung eine Härtung der Änderungskontrolle zu implementieren (postalisch versandter Code an die alte Adresse bei jeder E-Mail-/Telefonänderung; erzwungene Abkühlungsphasen; manuelle Überprüfung von Änderungen zu ProtonMail-Konten, die nach November 2022 erstellt wurden), trotz Beweisen für E-Mail-Übernahmemuster gegen Antragsteller; und (viii) es versäumte, Darknet-Überwachung und Look-alike-Takedowns einzusetzen, die auf FTX/Kroll-Forderungsschlüsselwörter ausgerichtet waren, nachdem Angebote von Antragsstellerdatensätzen online beobachtet wurden.

48. Die Risiken, die Kroll schuf und nicht minderte, waren vorhersehbar: Bundesgerichte in Krypto-Fällen hatten die PII von Kunden versiegelt, um Phishing- und „Wrench“-Angriffe zu verhindern; Bundesstrafverfolgungs- und Sicherheitsrichtlinien warnen Inhaber digitaler Vermögenswerte davor, 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. Krolls Handlungen und Unterlassungen waren die direkte und unmittelbare Ursache für die Schäden des Klägers und der Mitglieder der Sammelklägergruppe. Ohne Krolls Sicherheitsversäumnisse, die reine E-Mail-Benachrichtigung, die Weigerung, für die Fristen des 130. Omnibus-Einspruchs und die Frist für das Steuerformular Post zu versenden, und das fehlerhafte, abhängige Portal hätten der Kläger und viele Mitglieder der Sammelklägergruppe die Verifizierung rechtzeitig begonnen und abgeschlossen und Steuerformulare eingereicht; ihre Forderungen wären nicht gestrichen 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) Streichung/Verfall von Forderungen im Zusammenhang mit versäumten Verifizierungs-/Steuerformularfristen; (d) Auslagen (Überwachung, Geräte-/Wallet-Härtung, Dokumentenbeschaffung) und Zeitverlust; und (e) verminderte Privatsphäre und fortgesetzter Identitäts- und Vermögensdiebstahl.

51. Der Kläger und die Sammelklägergruppen fordern Schadensersatz und Folgeschäden in einer bei der Verhandlung nachzuweisenden Höhe, zusammen mit Zinsen vor und nach dem Urteil.

KLAGEGRUND II

Texas Deceptive Trade Practices—Consumer Protection Act (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 an Gläubiger gerichteten 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 aus seiner Forderung zu ermöglichen.

53. Kroll beging täuschende Handlungen, einschließlich: (1) der Darstellung, dass Dienstleistungen Eigenschaften/Vorteile hätten, die sie nicht hatten – nämlich, dass keine sensiblen PII (z. B. vollständiger Name, Postanschrift, Geburtsdatum, Wallet-/Transaktionsdetails) entwendet wurden und dass E-Mail-Prozesse nach der Datenschutzverletzung sicher seien; (2) des Versäumnisses, zum Zeitpunkt der Transaktionen bekannte Informationen offenzulegen (dass sensible PII in „unstrukturierten Daten“ vorhanden waren; dass Imitations-/E-Mail-Änderungs-Übernahmen aktiv waren), um Antragsteller zu verleiten, den reinen E-Mail-Workflow 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. Nach einem bekannten Sicherheitsvorfall und einer laufenden Phishing-Kampagne war das Beharren auf einer reinen E-Mail-Benachrichtigung für rechtskritische Fristen und das Unterlassen einer postalischen Sicherung 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 die wesentliche Ursache 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 PII.

56. Kroll handelte wissentlich und in mancher Hinsicht vorsätzlich: Es wusste aus seinen eigenen Untersuchungen in anderen Insolvenzmassen (z. B. BlockFi), dass sensible PII in „unstrukturierten Daten“ existierten, teilte den Antragstellern jedoch etwas anderes mit und passte die Benachrichtigungen und Arbeitsabläufe nicht entsprechend an.

57. Der Kläger fordert wirtschaftlichen Schadensersatz, Anwaltskosten, 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 einer einstweiligen Verfügung nicht möglich war, beantragt der Kläger, dass das Gericht die DTPA-Klage für 60 Tage ab Zustellung aussetzt, um Vergleichsgespräche gemäß den gesetzlichen Bestimmungen zu ermöglichen.

KLAGEGRUND III

Unlautere täuschende Handlungen nach New Yorker Recht (hilfsweise)

59. Kroll beging verbraucherorientierte täuschende Handlungen und Praktiken, einschließlich des Versands täuschender, öffentlich zugänglicher Fallmitteilungen und Antragstellerkommunikationen, der Verharmlosung der Datenschutzverletzung (Angabe, keine sensiblen PII), des Versäumnisses, wesentliche Fakten offenzulegen (PII 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 tatsächlichen Schadensersatz, gesetzlichen Schadensersatz, angemessene Anwaltskosten und einen Unterlassungsanspruch gemäß New York General Business Law §§ 349(h) und 350-e.

KLAGEGRUND IV

Grobe Fahrlässigkeit

60. Krolls Verhalten war mehr als gewöhnliche Fahrlässigkeit. In dem Wissen, dass die PII von Antragstellern offengelegt worden waren, und in dem Wissen, dass Antragsteller aktiv von Phishing betroffen waren, beharrte Kroll bewusst auf reinen E-Mail-, linklastigen, nachahmungsanfälligen Nachrichten für rechtsbeeinflussende Fristen; weigerte sich, in großem Umfang auf den Postweg umzusteigen, obwohl es die Fähigkeit dazu hatte und Post für andere kritische Mitteilungen verwendet hatte; und fuhr fort, die Einreichung von Steuerformularen von einem unzuverlässigen Forderungsportal abhängig zu machen, 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 Antragsstellerdaten dokumentiert hatten.

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

KLAGEGRUND V

Verletzung eines konkludenten Vertrags (Datenschutz & Forderungsverwaltung)

64. Durch die Anforderung und Annahme der PII und Forderungsanmeldungen des Klägers und der Mitglieder der Sammelklägergruppe und durch die Verpflichtung, das FTX-Portal (KYC/Prüfung) und Krolls EPOC (Forderungsanmeldung) zu nutzen, um am Insolvenzforderungsverfahren teilzunehmen, schloss Kroll konkludente 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 darauf ausgelegt sind, sicherzustellen, dass Antragsteller rechtsbeeinflussende Schritte abschließen können.

65. Der Kläger und die Mitglieder der Sammelklägergruppe leisteten, indem sie genaue Informationen lieferten und Krolls Anweisungen befolgten. Sie erwarteten vernünftigerweise, dass Kroll ihre Daten schützen und einen funktionalen, sicheren Prozess zur Durchführung der Verifizierung und zum Hochladen von Steuerformularen bereitstellen würde.

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

67. Als direkte und unmittelbare Folge erlitten der Kläger und die Mitglieder der Sammelklägergruppe

die oben beschriebenen Schäden, einschließlich Phishing-Verlust, Zeitwert- und Ausschüttungsschäden und Auslagen.

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

KLAGEGRUND 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 PII von Antragstellern und die Verwaltung des Verifizierungs-/Steuerformular-Workflows und der rechtsbeeinflussenden Mitteilungen.

70. Kroll führte diese übernommene Aufgabe fahrlässig aus, indem es nach der Datenschutzverletzung eine reine E-Mail-Benachrichtigung verwendete; sich weigerte, für die Fristen des 130. Omnibus-Einspruchs und die Frist für das Steuerformular Post zu versenden; die Einreichung von Steuerformularen von einem unzuverlässigen, statusabhängigen Arbeitsablauf abhängig machte; und es versäumte, einen alternativen Weg oder postalische Bestätigungen bereitzustellen.

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

72. Der Kläger und viele Mitglieder der Sammelklägergruppe verließen sich auf Krolls übernommene Aufgabe – sie nutzten das FTX-Portal und Krolls Antragstellerkommunikation/EPOC 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.

KLAGEGRUND VII

Fahrlässige Benachrichtigung und Forderungsbearbeitung nach der Datenschutzverletzung

74. Nach dem Vorfall vom 19. August 2023 hatte Kroll eine erhöhte Pflicht, vorhersehbare Schäden zu mindern und Benachrichtigungs- und Verfahrensanpassungen 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 des allgegenwärtigen Phishings und der Spam-Filterung, die auf Kroll-ähnliche E-Mails abzielten – und indem es versäumte, für die wichtigsten Mitteilungen auf den Postweg umzusteigen, einschließlich der Fristen für den 130. Omnibus-Einspruch 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 auf „Ausgesetzt/Unverifiziert“ zurück, 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 Streichung und das Steuerformular näher rückten.

78. Kroll stellte fälschlicherweise dar, dass keine sensiblen PII betroffen seien, und räumte später in einer anderen Krypto-Insolvenzmasse (BlockFi) das Vorhandensein von Geburtsdaten in „unstrukturierten Daten“ ein, wodurch die Wachsamkeit verringert und der Erfolg von Phishing-Angriffen erhöht wurde.

79. Als direkte und unmittelbare Folge von Krolls fahrlässiger Benachrichtigung und Forderungsbearbeitung versäumten oder konnten der Kläger und die Mitglieder der Sammelklägergruppe die Verifizierungs- und Steuerformularanforderungen, die sie sonst erfüllt hätten, nicht erfüllen, erlitten Phishing-Verluste und trugen Zeitwert- und Verwaltungsschäden.

80. Der Kläger und die Sammelklägergruppen fordern Schadensersatz für diese Verletzungen und eine Feststellung, dass Krolls Benachrichtigungs-/Bearbeitungspraktiken nach der Datenschutzverletzung unter den gegebenen Umständen unangemessen und rechtswidrig waren.

81. Der Kläger und die Sammelklägergruppen beantragen ferner eine einstweilige Verfügung, die eine mehrkanalige Benachrichtigung (E-Mail und First-Class Mail mit getippten URLs/eindeutigen Codes), postalische Bestätigungen für jede rechtsbeeinflussende Statusänderung, definierte Heilungsfristen vor der Streichung und einen manuellen/alternativen Kanal für die Verifizierung und die Einreichung von Steuerformularen vorschreibt. Kroll verwaltet weiterhin die an Gläubiger gerichtete Kommunikation und die Aufzeichnungen in Bezug auf diese Insolvenzmassen, sodass das Risiko zukünftiger Schäden ohne gerichtlich angeordnete Schutzmaßnahmen fortbesteht.

KLAGEGRUND VIII

Fahrlässige Falschdarstellung (Aussagen zum Prozess nach der Datenschutzverletzung)

82. Kroll stellte in Mitteilungen nach der Datenschutzverletzung 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 administrativer Berater 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 ließ dabei die angemessene Sorgfalt außer Acht. Der Kläger und die Mitglieder der Sammelklägergruppe verließen sich berechtigterweise darauf, indem sie mit demselben fehlerhaften Arbeitsablauf fortfuhren und auf Eskalationsalternativen verzichteten, was zu versäumten Fristen, Zeitwertverlusten und Streichungen führte.

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

KLAGEGRUND IX

Ungerechtfertigte Bereicherung (hilfsweise)

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

86. Es wäre ungerecht, 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 wiedereröffnete 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 Restitution und Herausgabe unrechtmäßig erlangter Vorteile sowie Gebührenverrechnungen, die den verursachten Schäden entsprechen.

KLAGEGRUND X

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

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

90. Der Kläger beantragt eine Feststellung, dass Krolls reine E-Mail-Benachrichtigung und das abhängige Portal nach der Datenschutzverletzung unter den gegebenen Umständen unangemessen waren und dass Kroll künftig Verfahren 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 Änderung des Verifizierungsstatus und eine

Mindestheilungsfrist von 30 Tagen vor Streichung oder Verfall; (c) Härtung der Änderungskontrolle: postalisch versandte Einmalcodes an die bestehende Postanschrift, bevor eine E-Mail-/Telefonänderung wirksam wird; (d) eine 14-tägige Abkühlungsphase für Änderungen der Kontaktmethode, es sei denn, sie wird durch einen postalisch versandten Code verifiziert; (e) manuelle Überprüfung von Wechseln zu kürzlich erstellten ProtonMail- oder anderen Hochrisikodomänen; (f) eine manuelle/alternative Methode zur Durchführung der Verifizierung und zur Einreichung von W-9/W-8BEN, die nicht von Portal-Flags abhängig ist, mit einem veröffentlichten Eskalations-SLA (5 Werktage Eskalation; 10 Werktage Lösung); (g) unveränderliche Audit-Protokolle von Statusänderungen und eine manuelle Übersteuerungsmöglichkeit; (h) branchenübliche Zustellbarkeits- und Anti-Spoofing-Kontrollen (dedizierte Domänen, DMARC/SPF/DKIM-Durchsetzung, Link-Tracking-Disziplin, Look-alike-Domänen-Takedowns, die auf FTX/Kroll/Forderungs-Schlüsselwörter ausgerichtet sind); (i) unabhängige jährliche Audits der Sicherheit, Zustellbarkeit und des Portal-Workflows 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 Interessenabwägung 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 Streichung aufgrund fehlerhafter Prozesse zu erhalten.

95. Der Kläger und die Sammelklägergruppen fordern auch ihre angemessenen Anwaltskosten und -gebühren, soweit gesetzlich zulässig, einschließlich unter den Doktrinen des gemeinsamen Fonds/ gemeinsamen Nutzens 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 Zustimmung zur Datenverarbeitung von FTX; 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 gerichtlich angeordneten Verwaltungs- und Datensicherheitspflichten (M365-Verletzung; Benachrichtigungskanäle nach der Verletzung; Fehlen eines nicht abhängigen 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 bundesstaatlichen Formulars 410 verfahrensrechtlich unzumutbar; und nach der öffentlichen Ordnung von New York kann grobe Fahrlässigkeit nicht vertraglich ausgeschlossen werden. Die Formulierung „auf individueller Basis“ in den Bedingungen ist auf das Schiedsverfahren beschränkt; es gibt keinen eigenständigen Sammelklageverzicht 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 Nichtunterzeichnerhaftung untergräbt.

KLAGEANTRAG

DAHER beantragt der Kläger, im eigenen Namen und im Namen der anderen Mitglieder der in dieser Klageschrift vorgeschlagenen Sammelklägergruppen, dass das Gericht zu ihren Gunsten und gegen die Beklagte wie folgt urteilt:

A. Für eine Anordnung, die diese Klage als Sammelklage zertifiziert und den Kläger und seinen Anwalt zur Vertretung der Sammelklägergruppen bestellt;

B. Für eine billigkeitsrechtliche Anordnung, die die Restitution und Herausgabe der Einnahmen

verlangt, die aufgrund des rechtswidrigen Verhaltens der Beklagten unrechtmäßig einbehalten wurden;

C. Für die Zuerkennung von tatsächlichem Schadensersatz, kompensatorischem 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: wirtschaftlicher Schadensersatz, dreifacher Schadensersatz für wissentliche/vorsätzliche Verstöße und angemessene und notwendige Anwaltskosten (DTPA § 17.50(d));
F. New York GBL §§ 349/350 (hilfsweise): gesetzlicher Schadensersatz und Anwaltskosten;

G. Für die Zuerkennung von Anwaltskosten und -gebühren sowie sonstigen Auslagen, einschließlich Sachverständigenhonoraren;
H. Zinsen vor und nach dem Urteil auf alle zugesprochenen Beträge; und

I. Solche weiteren und anderen 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 State Bar No. 24069863 nhall@hallattorneys.com
P.O. Box 1370
Edna, Texas 77957
+1 713 428 8967

ANWALT FÜR DEN KLÄGER UND DIE MUTMASSLICHEN SAMMELKLÄGERGRUPPEN