

& IMPORTANT DISCLAIMER

IMPORTANT DISCLAIMER

This document was translated from English to Dutch by InstaLaw using Google Gemini 2.5 Pro AI.

- AI translations may contain errors or inaccuracies
- This is NOT legal advice and creates NO attorney-client relationship
- The original English document is the only authoritative version
- For legal matters, consult a qualified attorney

Translation Date: 2025-08-20

Model: Google Gemini 2.5 Pro

Prompt: "Translate the following legal document from English to Dutch, do not make omissions, do not fabricate falsehoods."

TRANSLATED DOCUMENT

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

JACOB KEVYN REPKO, individueel en namens alle anderen in een vergelijkbare positie,

Eiser,

v.

KROLL RESTRUCTURING

ADMINISTRATION LLC (f/k/a Prime Clerk LLC),

Gedaagde.

)

) Zaaknr.: 1:25-cv-01319

)

)

) DAGVAARDING IN EEN GROEPSVORDERING

)

)

)

) JURYRECHTSPRAAK GEËIST

)

)

)

DAGVAARDING IN EEN GROEPSVORDERING

Eiser Jacob Kevyn Repko ("Eiser"), individueel en namens alle anderen in een vergelijkbare positie, stelt hierbij, via ondergetekende raadsman, het volgende tegen Gedaagde Kroll Restructuring Administration LLC (f/k/a Prime Clerk LLC) ("Kroll" of "Gedaagde"). Gebaseerd op persoonlijke kennis alsmede op informatie en overtuiging, stelt Eiser specifiek het volgende:

AARD VAN DE VORDERING

1. Dit is een groepsvordering wegens een datalek en nalatige administratie, voortvloeiend uit het beveiligingsincident van Kroll op 19 augustus 2023 en haar daaropvolgende falen om met redelijke zorg de op schuldeisers gerichte processen en kennisgevingen te beheren in drie grote cryptofaillissementen—FTX, BlockFi en Genesis.

2. Het datalek van Kroll legde (onder andere velden) namen, adressen, e-mailadressen, telefoonnummers, vorderingsidentificaties/-bedragen en kopieën van bewijzen van schuldvordering bloot—precies de metadata die criminelen misbruiken om cryptoslachtoffers te targeten met phishing- en "wrench"-aanvallen.

3. Na het datalek bleef Kroll volharden in het uitsluitend per e-mail versturen van kritieke kennisgevingen (inclusief FTX's 130e Omnibusbezwaar, vorderingsverificatie en deadlines voor belastingformulieren), ondanks (a) wijdverspreide phishing-imitaties die veel schuldeisers hadden geleerd om het openen van "Kroll"-e-mails te vermijden en (b) Kroll's

aangetoonde vermogen om brieven per eersteklas USPS-post te versturen wanneer zij daarvoor koos—bijvoorbeeld in Genesis, waar Kroll kennisgevingen van het datalek per First Class Mail verstuurde. 4. Federale faillissementsrechtbanken hadden de PII van schuldeisers verzegeld, juist om misdaden gericht op cryptobezitters te voorkomen—verwijzend naar de reële schade die werd gezien in het Celsius-faillissement (phishing- en "wrench"-aanvallen). Het Genesis-dossier legt deze zorgen vast in bevelen tot verzegeling van klantinformatie. 5. Eiser Jacob Kevyn Repko (Dripping Springs, Texas) diende een vordering als klant van FTX in en ontving vervolgens de kennisgeving van het datalek van Kroll op 24 augustus 2023. Zijn PII en vorderingsgegevens behoorden tot de gecompromitteerde data. 6. In de maanden die volgden, functioneerde het FTX Customer Claims Portal (het "FTX-portaal") herhaaldelijk niet naar behoren: de KYC van Eiser stond op "Geverifieerd", maar sprong vervolgens terug naar "In de wacht/ Niet-geverifieerd", waardoor hij het IRS-formulier (W-9) dat vereist is om uitkeringen te ontvangen, niet kon uploaden, ondanks tientallen support-e-mails. 7. Omdat het FTX-portaal het uploaden van belastingformulieren afhankelijk maakt van "KYC Geverifieerd", kan Eiser de laatste voorwaarden niet voltooien; onder het bekrachtigde plan en de trustcommunicatie kunnen vorderingen worden geschrapt of uitkeringen verbeurd worden verklaard als belastingformulieren niet tijdig worden geüpload. 8. Eiser leed ook direct verlies door phishing na het datalek: hij maakte 1,9 ETH over van een exchange-account naar zijn hot wallet om 12:43 PM op 3 juli 2025, en dit werd omgeleid via een geautomatiseerde transactiebot die vaak wordt gebruikt om lopende overdrachten te onderscheppen naar een wallet die niet door Eiser wordt beheerd, wat overeenkomt met Kroll's eigen waarschuwing dat aanvallers de gelekte gegevens zouden gebruiken om crypto-accounts te phishen.

PARTIJEN 9. Eiser Jacob Repko is een natuurlijk persoon, woonachtig in Hays County, Texas. Hij is een klant-schuldeiser van FTX met een opgenomen vordering van \$87.487,93.

10. Gedaagde Kroll Restructuring Administration LLC is een LLC uit Delaware met aanzienlijke activiteiten in het hele land, inclusief kantoren in Texas.

11. Op basis van informatie en overtuiging daagt Eiser ook Gedaagden 1-5, momenteel niet-geïdentificeerde entiteiten die geen deel uitmaken van Kroll en die, indien van toepassing, hebben deelgenomen aan de op de eiser gerichte verificatie of de inname van belastingformulieren (inclusief externe KYC-leveranciers). Voor zover een entiteit die geen deel uitmaakt van Kroll de KYC-statusvlaggen of de afhankelijkheid van W-9/W-8-formulieren binnen het FTX-portaal controleerde, voert Eiser die stellingen subsidiair aan en zal hij de ware namen wijzigen en vervangen wanneer deze worden geïdentificeerd. Indien Kroll een verantwoordelijke derde partij aanwijst, zal Eiser deze partij tijdig voegen onder de regels voor proportionele aansprakelijkheid van Texas.

RECHTSMACHT EN BEVOEGDE RECHTBANK

12. Deze Rechtbank heeft materiële rechtsmacht op grond van 28 U.S.C. § 1332(d) (CAFA): de voorgestelde groepen overschrijden 100 leden; de totale geschilwaarde overschrijdt \$5.000.000; er bestaat minimale diversiteit (eiser uit Texas versus gedaagde uit Delaware/New York met groepsleden uit het hele land/internationaal).

13. Deze Rechtbank heeft personele rechtsmacht over Kroll omdat Kroll kantoren onderhoudt in Austin, Dallas en Houston, doelbewust administratie-/kennisgevingswerk en communicatie met eisers richt op Texas, en handelingen heeft verricht die schade hebben veroorzaakt aan een inwoner van Texas in dit District. De vorderingen van Eiser vloeien voort uit of houden verband met dat gedrag in dit forum, en het uitoefenen van rechtsmacht is in overeenstemming met een eerlijk proces.

14. De rechtbank is bevoegd op grond van 28 U.S.C. § 1391(b) omdat een wezenlijk deel van de gebeurtenissen en de schade in dit District heeft plaatsgevonden: Eiser woont hier, ontving hier de kennisgevingen van Kroll, gebruikte hier het FTX Customer Claims Portal (claims.ftx.com) en vervolgens

Kroll's Elektronisch Bewijs van Schuldvordering ("EPOC"), en leed hier schade door phishing.

15. Op dit moment stelt Eiser geen vorderingen in tegen de Debiteuren, of enige door het plan gevrijwaarde partij, en zoekt hij geen rechtsmiddel dat interpretatie, wijziging of handhaving van het Plan of het Bekrachtigingsbevel vereist. Dit zijn onafhankelijke vorderingen uit onrechtmatige daad/contract tegen de niet-debiteur Kroll. Deze actie is geen kernprocedure; Eiser eist een jury en stemt niet in met faillissementsrechtspraak.

DEFINITIES

16. "FTX Customer Claims Portal" of "FTX-portaal" betekent het portaal op claims.ftx.com dat wordt beheerd voor de Debiteuren/FTX Recovery Trust (met leveranciers) om KYC/AML en accountbeoordeling af te handelen. "Kroll-site" betekent de website van Kroll, inclusief de EPOC-interface op restructuring.ra.kroll.com, die Faillissementsformulier 410-inzendingen ontving en het openbare vorderingenregister bijhield. Waar de controle onduidelijk is, voert Eiser subsidiair aan tegen Gedaagde Does die zullen worden vervangen wanneer geïdentificeerd.

FEITELIJKE STELLINGEN

A. Het datalek van Kroll omvatte FTX, Genesis en BlockFi

17. Op of omstreeks 19 augustus 2023 voerde een aanvaller een SIM-swap uit op de telefoon van een Kroll-medewerker, waardoor hij toegang kreeg tot de cloudbestanden van Kroll met eisersgegevens voor elke faillissementsboedel. Onafhankelijke dreigingsinformatie bevestigt dat de gecompromitteerde velden later te gelde werden gemaakt en geoperationaliseerd door fraudeurs die zich richtten op FTX-eisers en transacties op de secundaire markt.

18. Kroll's indiening bij Genesis geeft toe dat de getroffen gegevens namen, telefoonnummers, adressen, vorderingsnummers/-bedragen, wallet-/muntensaldi en kopieën van bewijzen van schuldvordering omvatten.

19. De kennisgeving van BlockFi geeft verder aan dat geboortedatum, postadres en rijbewijsnummers betrokken waren en beschrijft Kroll's vertraagde identificatie van een grote hoeveelheid "Ongestructureerde Bestanden".

B. Rechtbanken verzegelden PII van schuldeisers omdat cryptoschuldeisers te maken hebben met unieke aanvalsvectoren

20. In Genesis vaardigde de rechtbank verzegelingsbevelen uit ter bescherming van de namen/contactgegevens van schuldeisers, verwijzend naar de Celsius-ervaring waar phishing- en wrench-aanvallen volgden op openbare bekendmakingen.

C. Kroll wist dat e-mail onveilig was, maar verzuimde post te gebruiken voor kritieke kennisgevingen

21. Op basis van informatie en overtuiging waarschuwde Kroll de Genesis-schuldeisers publiekelijk voor phishing en stuurde het kennisgevingen van het datalek per First-Class Mail om de bezorging te garanderen.

22. Toch vertrouwde Kroll in het geval van FTX, voor even (of meer) gevolgenrijke kennisgevingen—inclusief de deadlines voor het 130e Omnibusbezwaar (bijv. start KYC voor 1 maart 2025; voltooi voor 1 juni 2025) en de deadline voor het belastingformulier—voornamelijk op e-mail, slechts enkele maanden na haar eigen datalek dat phishing veroorzaakte, wetende dat veel ontvangers "Kroll"-e-mails niet zouden openen uit angst voor oplichting of ze in hun spam-/junkmap zouden vinden. Openbare dreigingsinformatie toont accountovernames door phishing waarbij daders de e-mailadressen van eisers veranderden in nieuwe ProtonMail-adressen en snel 2FA-uitdagingen doorstonden—precies de aanval die Kroll's aanpak van uitsluitend e-mail niet-gemitigeerd liet.

23. Het FTX-portaal maakt het uploaden van W-9/W-8BEN afhankelijk van KYC-verificatie. Wanneer het portaal een gebruiker ten onrechte terugzet naar "In de wacht/Niet-geverifieerd", wordt de stap van het belastingformulier onmogelijk—wat het risico met zich meebrengt van schrapping van de vordering of verbeurdverklaring van uitkeringen onder de planprocessen die aan schuldeisers zijn gecommuniceerd. In een omgeving waar eisers zijn getraind om 'Kroll'-e-mails te vermijden vanwege actieve imitatie, was een afhankelijke, uitsluitend online stap voor het belastingformulier zonder een terugvaloptie via First-Class Mail niet redelijkerwijs berekend om op de hoogte te stellen of voltooiing mogelijk te maken.

24. Het bekrachtigingsbevel van FTX bepaalt uitdrukkelijk dat Kroll niet wordt gevrijwaard of geëxcuseerd voor vorderingen met betrekking tot het "Beveiligingsincident" en dat de schade van klanten

die in een andere procedure verhaalbaar is, niet wordt beperkt door de uitkeringen van het plan. Eiser verzoekt de rechtbank respectvol om gerechtelijke kennisneming van dat uittreksel van het bekrachtigingsbevel op grond van Fed. R. Evid. 201.

25. Naast te zijn aangesteld door de faillissementsrechtbank onder §156(c) voor kennisgevingen, werd Kroll ingehuurd als Administratief Adviseur om faillissementsadministratiediensten uit te voeren onder haar opdrachtdocumenten en het aanstellingsbevel van de Rechtbank. Deze op schuldeisers gerichte taken (werving/stemming/telling en afhandeling van communicatie met eisers) ondersteunen de administratieve verplichtingen die hierin worden gesteld.

D. De ervaring van Eiser

26. Eiser diende zijn vordering als klant in via het FTX-portaal en, toen daarom werd gevraagd, diende hij het faillissementsformulier 410 in via Kroll's EPOC.

27. Hij ontving de kennisgeving van het datalek van Kroll waarin de blootstelling van zijn naam, adres, e-mail en rekeningssaldo werd bevestigd en werd gewaarschuwd voor phishing gericht op crypto-activa.

28. Na te hebben geworsteld met portaalblokkades en vertragingen, werd de KYC van Eiser geverifieerd op of rond 3 november 2023, maar het portaal keerde later terug naar "In de wacht", waardoor het uploaden van het IRS-formulier werd geblokkeerd; talloze e-mails naar Kroll bleven onopgelost.

29. Na het datalek werd Eiser het slachtoffer van phishing: 1,9 ETH werd binnen enkele minuten na aankomst in zijn hot wallet leeggehaald (aankomst om 12:43 PM; uitgaand naar het adres van de aanvaller om 12:49 PM).

30. Eiser heeft een opgenomen FTX-vordering van \$87.487,93 en wordt nu geconfronteerd met het verlies van een deel of de gehele waarde van de uitkering omdat hij niet kan voldoen aan de voorwaarden van het plan vanwege storingen in het portaal en falende kennisgevingen.

31. Eiser leed concrete schade, waaronder: (a) daadwerkelijk misbruik—diefstal van 1,9 ETH binnen enkele minuten na aankomst in zijn wallet op 3 juli 2025; (b) schade door tijdswaarde en uitkeringschade door geblokkeerde verificatie/indiening van belastingformulieren; (c) uit eigen zak betaalde mitigatiekosten; (d) verlies van privacy/controle over PII; en (e) een aanzienlijk risico op toekomstig misbruik gezien de hierin gedocumenteerde patronen van crypto-targeting.

E. Systematisch misbruik van gelekte eisersgegevens

32. Voorzienbaarheid is geen abstractie: onderzoekers traceerden \$5,6 miljoen aan fraude door misbruik van FTX-vorderingsgegevens, inclusief verkopen op het dark web van datasets van eisers en patronen van e-mailwijziging/2FA-omzeiling—precies de schade die rechtbanken probeerden te voorkomen door de PII van cryptoschuldeisers te verzegelen. Kroll's tegenstrijdige berichtgeving dat er geen gevoelige PII in gevaar was, misleidde consumenten over de noodzaak om elke "Kroll"-e-mail als verdacht te behandelen en om een back-up per post te eisen.

33. Onafhankelijke dreigingsinformatie bevestigt dat FTX-eisersgegevens actief zijn ingezet tegen schuldeisers en tegenpartijen. In juli-november 2024 documenteerden onderzoekers minstens \$5,6 miljoen aan fraude in verband met de handel in FTX-vorderingen, waarbij een actor (of groep) zich voordeed als vorderinghouders met behulp van door AI bewerkte selfies, nieuwe ProtonMail-accounts en vervalste identificatie.

34. De werkwijze van de actor omvatte: (a) recent aangemaakte ProtonMail-adressen die het oorspronkelijke e-mailadres van de eiser vervingen; (b) snelle invoer van 2FA-codes, wat duidt op accountovername; en (c) witwassen via stortingsadressen van Gate.io, CoinEx en Binance. Deze patronen zijn consistent met de compromittering van inloggegevens door phishing na het Kroll-incident.

35. Hetzelfde onderzoek toont aan dat FTX-vorderingsgegevens werden geadverteerd op dark-webforums, inclusief namen, telefoonnummers, e-mails, wallet-/transactiegegevens en andere aan de vordering gekoppelde gegevens—de exacte velden waarvan Kroll erkende dat ze waren gecompromitteerd (namen, e-mails, telefoonnummers, postadressen, accountidentificaties en saldi, en in sommige gevallen geboortedata).

36. Onderzoekers observeerden ook e-mailwijzigingen naar ProtonMail-accounts die na de sluiting waren aangemaakt voor vorderingen die oorspronkelijk met andere e-mails waren geopend, wat duidt op overname en imitatie van eisersaccounts.

37. Het rapport documenteert blockchain-paden van de wallets van de imitator naar stortingsadressen van CoinEx en identificeert een tussenliggende wallet die geassocieerd wordt met geautomatiseerde

transactieactiviteit; het merkt interacties op met Amerikaanse exchanges (Coinbase en Kraken) die kunnen worden gedagvaard voor KYC. Dit bewijst een samenhangend, herhaalbaar fraudepatroon dat misbruik maakt van de PII van eisers en zwakheden in de workflow.

38. Het rapport merkt verder een "Orbeon Forms – Page Not Found"-fout op die naar voren kwam tijdens een due-diligence-doorloop van het FTX-portaal—consistent met een kwetsbare workflow voor eisers en foutstatussen die kwaadwillenden kunnen nabootsen, wat de verwarring in een omgeving met veel phishing versterkt.

F. Onjuiste voorstellingen en weglatingen na het datalek

39. Kroll bagatelliseerde publiekelijk en in communicatie met eisers de omvang van het datalek—en stelde aanvankelijk dat er geen gevoelige PII was gecompromitteerd. In andere boedels die het beheerde (bijv. BlockFi), maakte Kroll later bekend dat geboortedata waren opgenomen in "ongestructureerde data", wat haar eerdere verklaringen tegensprak. Kroll vertelde FTX-eisers eveneens dat ze konden blijven communiceren via op e-mail gebaseerde workflows en waarschuwde niet dat kwaadwillenden Kroll imiteerden en e-mailadressen van eisers veranderden in nieuw aangemaakte ProtonMail-accounts om 2FA te omzeilen—patronen bevestigd door onafhankelijke dreigingsinformatie. Deze verklaringen en weglatingen waren materieel, op consumenten gericht en misleidend, en ze brachten redelijke eisers ertoe het risico te onderschatten, uitsluitend e-mailkanalen te blijven gebruiken en krachtiger herstel uit te stellen, wat bijdroeg aan phishingverlies, schade door tijdswaarde en gemiste deadlines die resulteerden in geschrapte vorderingen.

STELLINGEN MET BETREKKING TOT DE GROEPSVORDERING

40. Wereldwijde Groep van Cryptoschuldeisers: Alle personen wereldwijd wier PII of vorderingsgegevens die aan Kroll zijn verstrekt voor de faillissementszaken van FTX, BlockFi of Genesis zijn benaderd, geëxfiltreerd of redelijkerwijs in gevaar waren bij het Kroll-incident van augustus 2023. Het lidmaatschap van de groep is vaststelbaar aan de hand van de kennisgevingslijsten van Kroll, EPOC-gegevens en de vorderingenregisters van de boedels die personen identificeren wier gegevens volgens Kroll zijn benaderd of redelijkerwijs in gevaar waren bij het incident.

41. Subgroepen per Boedel: (a) FTX Subgroep; (b) BlockFi Subgroep; en (c) Genesis Subgroep.

Eiser zal benoemde vertegenwoordigers voor de BlockFi- en Genesis-subgroepen toevoegen op of vóór de certificering van de groep. 42. Subgroepen per Schade (over de boedels heen): (i) Subgroep phishing/cryptoverlies; (ii) Subgroep portaal/verificatie/belastingformulier (verlies door schrapping, verlies van tijdswaarde en administratieve schade);

(iii) Standaard subgroep schade door datalek (inbreuk op privacy, mitigatiekosten). 43. Aan de eisen van aantal, gemeenschappelijkheid, typiciteit en geschiktheid is voldaan: gemeenschappelijke vragen omvatten of Kroll zorgplichten had en schond met betrekking tot gegevensbeveiliging, de adequaatheid van kennisgevingen en de administratie van het vorderingsproces; of kennisgeving uitsluitend per e-mail redelijk was na het datalek; en of een rechterlijk bevel gerechtvaardigd is.

RECHTSKEUZE

44. Gedragsregulerende normen worden beheerst door het recht van New York (Kroll heeft zijn hoofdkantoor en handelde vanuit NY), of subsidiair door het recht van Texas voor inwoners van Texas en schade in Texas. De vorderingen staan of vallen met plichten/handelingen die gemeenschappelijk zijn voor alle groepsleden. Kwesties van vatbaarheid voor arbitrage worden beheerst door de FAA; het openbare beleid van New York verbiedt contractuele vrijwaring voor grove nalatigheid.

GRONDEN VAN DE VORDERING

GROND I

Nalatigheid (recht van New York; subsidiair recht van Texas)

45. Kroll had jegens Eiser en de Groepen (FTX, BlockFi en Genesis) een zorgplicht om redelijke zorg te betrachten bij het verzamelen, opslaan, verzenden en beheren van PII en vorderingsgegevens van eisers; om een functionele verificatie-/belastingformulierworkflow te ontwerpen, te exploiteren en te ondersteunen; en—vooral na het incident van 19 augustus 2023—om kennisgevingen te doen die redelijkerwijs berekend waren, onder alle omstandigheden, om eisers op de hoogte te stellen van deadlines en stappen die hun rechten beïnvloeden en om voorzienbare phishing- en bezorgingsrisico's te mitigeren.

46. Die plichten vloeiden voort uit (a) de rollen van Kroll als door de rechtbank aangestelde agent voor kennisgevingen/vorderingen en Administratief Adviseur; (b) gerechtelijke bevelen tot verzegeling van de PII van cryptoschuldeisers vanwege bekende phishing- en fysieke veiligheidsrisico's; (c) Kroll's eigen kennis en waarschuwingen dat blootgestelde e-mailadressen van eisers het doelwit zouden zijn van phishing; en (d) Kroll's controle over de communicatie met eisers en de EPOC-inname; voor zover een entiteit die geen deel uitmaakt van Kroll de KYC-statusvlaggen en de afhankelijkheid van belastingformulieren binnen het FTX-portaal controleerde, voert Eiser die stellingen subsidiair aan tegen Gedaagde Does die zullen worden vervangen wanneer geïdentificeerd. Deze plichten zijn onafhankelijk van enig contract en worden erkend onder het recht van New York en Texas waar het gedrag van een partij een voorzienbaar risico op identiteits-/vermogensdiefstal creëert of verhoogt voor een bekende, eindige groep (cryptoeisers met verzegelde PII), en waar keuzes met betrekking tot kennisgeving en processen na een datalek worden beheerst door de beginselen van een eerlijk proces (bijv. Mullane; Jones v. Flowers) en de privacy-/kennisgevingsbevelen van de faillissementsrechtbank. 47. Kroll schond haar plichten door, onder andere: (i) het toestaan van de door SIM-swap mogelijk gemaakte compromittering van cloudopslagplaatsen met eisersgegevens; (ii) het niet onmiddellijk en volledig identificeren van alle getroffen gegevensopslagplaatsen; (iii) het volharden—na het datalek—in kennisgeving uitsluitend per e-mail voor communicatie die rechten beïnvloedt, ook al konden veel eisers legitieme Kroll-e-mails niet onderscheiden van phishing en ook al had Kroll de mogelijkheid en het precedent om First-Class Mail te sturen; (iv) het toestaan van een uitkeringsworkflow waarin het uploaden van W-9/W-8BEN werd geblokkeerd tenzij KYC "Geverifieerd" toonde in het FTX-portaal, terwijl er geen handmatige/alternatieve indieningsroute via Kroll's EPOC of per post/e-mail werd geboden; (v) het niet bieden van enige handmatige/alternatieve indieningsroute of per post verstuurd bevestigingen voor statuswijzigingen; (vi) het bieden van circulaire, vertraagde of ineffectieve ondersteuning die de schade verlengde en verergerde; (vii) het niet implementeren, na het datalek, van versterkte wijzigingscontroles (een code per post naar het oude adres sturen voor elke e-mail-/telefoonwijziging; gedwongen afkoelingsperiodes; handmatige beoordeling van wijzigingen naar ProtonMail-accounts die na november 2022 zijn aangemaakt) ondanks bewijs van patronen van e-mailovername tegen eisers; en (viii) het niet inzetten van dark-webmonitoring en het neerhalen van look-alike domeinen die zijn gekoppeld aan FTX/Kroll-vorderings sleutelwoorden nadat aanbiedingen van eisersdatasets online werden waargenomen. 48. De risico's die Kroll creëerde en niet wist te mitigeren, waren voorzienbaar: federale rechtbanken in cryptozaken hadden de PII van klanten verzegeld om phishing- en "wrench"-aanvallen te voorkomen; federale wetshandhavings- en veiligheidsrichtlijnen waarschuwen houders van digitale activa om identificerende informatie privé te houden; en Kroll zelf vertelde eisers dat aanvallers overtuigende e-mails zouden sturen om accounts en wallets over te nemen. Onder deze omstandigheden was uitsluitend e-mail voor stappen en deadlines die cruciaal zijn voor rechten niet redelijk.

49. De handelingen en nalatigheden van Kroll waren de directe en voorzienbare oorzaak van de schade van Eiser en de groepsleden. Zonder de beveiligingsfouten van Kroll, de kennisgeving uitsluitend per e-mail, de weigering om post te sturen voor de deadlines van het 130e Omnibusbezwaar en de deadline voor het belastingformulier, en het defecte, afhankelijke portaal, zouden Eiser en veel groepsleden de verificatie tijdig hebben gestart en voltooid en belastingformulieren hebben ingediend; zouden hun vorderingen niet zijn geschrapt of "in de wacht" zijn geplaatst, waardoor de uitkeringen van het plan werden vertraagd; en zouden zij phishingverliezen en mitigatiekosten hebben vermeden.

50. Eiser en de Groepen hebben schade geleden, waaronder, zonder beperking: (a) phishing-/cryptoverliezen (voor Eiser 1,9 ETH leeggehaald binnen enkele minuten na ontvangst); (b) schade door tijdswaarde door vertragingen in de uitkering veroorzaakt door kennisgeving uitsluitend per e-mail en de defecten van het portaal; (c) schrapping/verbeurdverklaring van vorderingen in verband met gemiste verificatie-/belastingformulierdeadlines; (d) uit eigen zak betaalde kosten (monitoring, verharding van apparaten/wallets, aanschaf van documenten) en verloren tijd; en (e) verminderde privacy en voortdurende identiteits- en vermogensdiefstal.

51. Eiser en de Groepen vorderen een compensatoire en gevolgschadevergoeding tot een op het proces te bewijzen bedrag, samen met wettelijke rente voor en na het vonnis.

GROND II

Wet op Misleidende Handelspraktijken en Consumentenbescherming van Texas (Tex. Bus. & Com. Code § 17.41 et seq.)

52. Eiser is een consument onder Tex. Bus. & Com. Code §17.45(4) omdat hij diensten zocht en gebruikte—de vorderingsadministratie van Kroll en de op schuldeisers gerichte diensten die ten behoeve van Eiser zijn ingekocht door de FTX Debiteuren/FTX Recovery Trust—en die diensten werden aan Eiser verleend om hem in staat te stellen zijn vordering te doen gelden en uitkeringen te ontvangen.

53. Kroll heeft zich schuldig gemaakt aan misleidende handelingen, waaronder: (1) het voorstellen dat diensten kenmerken/voordelen hadden die ze niet hadden—namelijk dat er geen gevoelige PII (bijv. volledige naam, postadres, geboortedatum, wallet-/transactiegegevens) was buitgemaakt en dat e-mailprocessen veilig waren na het datalek;

(2) het niet openbaar maken van informatie die bekend was op het moment van de transacties (dat gevoelige PII zich in "ongestructureerde data" bevond; dat imitatie/e-mailwijzigingsovernames actief waren) om eisers ertoe te bewegen de uitsluitend op e-mail gebaseerde workflow voort te zetten; en (3) het voorstellen van rechten/plichten onder het vorderingsproces die zij niet hadden—wat impliceert dat kennisgeving per e-mail alleen redelijk en voldoende was voor deadlines die cruciaal zijn voor rechten. 54. In de nasleep van een bekend beveiligingsincident en een actieve phishingcampagne was het volharden in kennisgeving uitsluitend per e-mail voor deadlines die cruciaal zijn voor rechten en het weglaten van een post-backup en een handmatige indieningskanaal voor belastingformulieren een onbillijke handelwijze die op grove wijze misbruik maakte van het gebrek aan kennis van eisers en hun onvermogen om zichzelf te beschermen. 55. De schendingen van de DTPA door Kroll waren de veroorzakende factor van de schade van Eiser, waaronder (i) de diefstal van 1,9 ETH na phishing, (ii) schade door tijdswaarde/uitkering door geblokkeerde verificatie en indiening van belastingformulieren, en (iii) mitigatiekosten en verlies van privacy/controle over PII. 56. Kroll handelde willens en wetens, en in sommige opzichten opzettelijk: het wist uit eigen onderzoek in andere boedels (bijv. BlockFi) dat gevoelige PII bestond in "ongestructureerde data", maar vertelde eisers anders en paste de kennisgeving en workflows niet dienovereenkomstig aan. 57. Eiser vordert economische schade, advocaatkosten, kosten en een drievoudige schadevergoeding voor willens en wetens/opzettelijke schendingen onder de Texas DTPA. 58. Eiser heeft de kennisgeving voorafgaand aan de rechtszaak verzonden of verzendt deze gelijktijdig. Voor zover kennisgeving niet haalbaar was vanwege dreigende verjaring en de noodzaak van een voorlopige voorziening, verzoekt Eiser de Rechtbank de DTPA-vordering op te schorten voor 60 dagen vanaf de betekening om besprekingen over herstel mogelijk te maken zoals wettelijk voorzien.

GROND III

Wet op Oneerlijke Misleidende Handelingen van New York (subsidiar) 59. Kroll heeft zich beziggehouden met op consumenten gerichte misleidende handelingen en praktijken, waaronder het verzenden van misleidende publiekgerichte zaakkennisgevingen en communicatie met eisers, het bagatelliseren van het datalek (door te stellen dat er geen gevoelige PII was), het niet openbaar maken van materiële feiten (PII aanwezig in bestanden en in "ongestructureerde data"; actieve imitatie), en het aanmoedigen van voortgezette communicatie uitsluitend per e-mail in een actieve phishingomgeving. Deze handelingen waren op een materiële manier misleidend en hebben Eiser schade berokkend. Eiser vordert daadwerkelijke schade, wettelijke schadevergoeding, redelijke advocaatkosten en een rechterlijk bevel op grond van New York General Business Law §§ 349(h) en 350-e.

GROND IV

Grove Nalatigheid

60. Het gedrag van Kroll was meer dan gewone nalatigheid. Wetende dat de PII van eisers was blootgesteld, en wetende dat eisers actief werden gephisht, volhardde Kroll bewust in uitsluitend op e-mail gebaseerde, link-zware, look-alike-gevoelige berichtgeving voor deadlines die rechten beïnvloeden; weigerde over te schakelen op post op grote schaal, ook al had het de mogelijkheid en had het post gebruikt voor andere kritieke communicatie; en bleef de indiening van belastingformulieren afhankelijk maken van een onbetrouwbaar vorderingenportaal dat gebruikers herhaaldelijk heen en weer schakelde tussen "Geverifieerd" en "In de wacht" zonder uitleg—zelfs nadat informatie van derden de voortdurende imitatie, overnames door e-mailwijziging en witwasroutes met behulp van eisersgegevens documenteerde.

61. Het falen van Kroll om voor de hand liggende waarborgen in te zetten—First-Class Mail voor kennisgevingen die cruciaal zijn voor rechten, per post verstuurde bevestigingen van statuswijzigingen, een handmatig, niet-afhankelijk pad voor belastingformulieren, versterking van wijzigingscontroles (codes per post naar het bestaande adres; afkoelingsperiodes; handmatige beoordeling van overschakelingen naar recent aangemaakte ProtonMail-accounts), en dark-webmonitoring—was een extreme afwijking van

de normale zorgvuldigheid in het licht van een hoge waarschijnlijkheid van ernstige schade aan een populatie wier PII juist was verzegeld om phishing en fysieke targeting te voorkomen.

62. Het grof nalatige gedrag van Kroll was een substantiële factor in het veroorzaken van de schade van Eiser en de Groepen en ondersteunt een toekenning van punitieve schadevergoeding om soortgelijk wangedrag te bestraffen en af te schrikken.

63. Eiser en de Groepen vorderen een punitieve schadevergoeding tot een bedrag dat voldoende is om de laakbaarheid van het gedrag van Kroll te weerspiegelen en toekomstige schendingen af te schrikken.

GROND V

Wanprestatie van een Stilzwijgend Contract (Privacy & Vorderingsadministratie)

64. Door de PII en vorderingsinzendingen van Eiser en de groepsleden te vragen en te accepteren en door hen te verplichten het FTX-portaal (KYC/beoordeling) en Kroll's EPOC (indiening van vordering) te gebruiken om deel te nemen aan het faillissementsvorderingsproces, is Kroll stilzwijgende overeenkomsten aangegaan om (a) die informatie met redelijke beveiliging te beschermen, (b) de verificatie- en belastingformulierstappen met redelijke zorg te beheren, en (c) kanalen te bieden die redelijkerwijs zijn ontworpen om ervoor te zorgen dat eisers stappen die hun rechten beïnvloeden, kunnen voltooien.

65. Eiser en de groepsleden hebben hun deel van de overeenkomst nagekomen door nauwkeurige informatie te verstrekken en de instructies van Kroll te volgen. Zij verwachtten redelijkerwijs dat Kroll hun gegevens zou beschermen en een functioneel, veilig proces zou bieden om de verificatie te voltooien en belastingformulieren te uploaden.

66. Kroll schond deze stilzwijgende beloften door ongeautoriseerde toegang tot eisersgegevens toe te staan; door door te gaan met het gebruik van kennisgevingen uitsluitend per e-mail in een bekende phishingomgeving; door te volharden in een defecte, afhankelijke workflow zonder een alternatief pad; en door geen handmatige, niet-afhankelijke indieningsoptie of per post verstuurde bevestigingen te bieden voor statuswijzigingen die rechten beïnvloeden.

67. Als direct en voorzienbaar gevolg hebben Eiser en de groepsleden de hierboven beschreven schade geleden, inclusief phishingverlies, schade door tijdswaarde en uitkering, en uit eigen zak betaalde kosten.

68. Eiser en de Groepen vorderen schadevergoeding, restitutie en alle andere passende rechtsmiddelen voor de wanprestatie van Kroll van het stilzwijgende contract.

GROND VI

Nalatige Uitvoering van een Taak (Restatement (Second) of Torts § 324A)

69. Kroll heeft zich ertoe verbonden diensten te verlenen waarvan het wist dat ze noodzakelijk waren voor de bescherming van Eiser en de Groepen—namelijk het beschermen van de PII van eisers en het beheren van de verificatie-/belastingformulierworkflow en kennisgevingen die rechten beïnvloeden.

70. Kroll heeft die taak nalatig uitgevoerd door na het datalek uitsluitend e-mail te gebruiken voor kennisgevingen; door te weigeren post te sturen voor de deadlines van het 130e Omnibusbezwaar en de deadline voor het belastingformulier; door de indiening van belastingformulieren afhankelijk te maken van een onbetrouwbare, status-afhankelijke workflow; en door geen alternatief pad of per post verstuurde bevestigingen te bieden.

71. De nalatige uitvoering door Kroll verhoogde het risico op schade voor Eiser en de groepsleden (gemiste of genegeerde kennisgevingen, blokkades door statuswisselingen, phishing) en was een substantiële factor in de daaruit voortvloeiende verliezen.

72. Eiser en veel groepsleden vertrouwden op de taakuitvoering van Kroll—door het FTX-portaal en de communicatie/EPOC van Kroll voor eisers te gebruiken zoals geïnstrueerd en andere stappen achterwege te laten omdat Kroll het exclusieve kanaal was voor verificatie en vorderingsadministratie.

73. Eiser en de Groepen hebben recht op schadevergoeding die direct is veroorzaakt door de nalatige taakuitvoering van Kroll.

GROND VII

Nalatige Kennisgeving en Vorderingsverwerking na het Datalek

74. Na het incident van 19 augustus 2023 had Kroll een verhoogde plicht om voorzienbare schade te mitigeren en om kennisgeving en procesaanpassingen te bieden die redelijkerwijs berekend waren om eisers te bereiken en tijdige naleving van stappen die rechten beïnvloeden mogelijk te maken.

75. Kroll schond die plicht door te blijven vertrouwen op kennisgeving uitsluitend per e-mail—ondanks wijdverspreide phishing en spamfiltering gericht op Kroll-look-alike e-mails—en door niet over te schakelen op post voor de meest gevolgenrijke communicatie, inclusief de deadlines van het FTX 130e Omnibusbezwaaar (te beginnen voor 1 maart 2025 en te voltooien voor 1 juni 2025) en de deadline voor het belastingformulier. Het bekrachtigde plan bevatte geen vaste data in de plantekst; daarom maakte de kanaalkeuze van Kroll die kennisgevingen doorslaggevend voor de uitkomst. Veel redelijke eisers openden Kroll-e-mails niet omdat dit aanvoelde als "Russische roulette" tijdens actieve phishingcampagnes; veel kennisgevingen belandden in junk-/spam-mappen en werden niet gezien. 76. Onafhankelijk daarvan exploiteerde FTX een portaal dat de indiening van W-9/W-8BEN blokkeerde tenzij "KYC Geverifieerd", maar het systeem zette geverifieerde gebruikers ten onrechte terug naar "In de wacht/Niet-geverifieerd", zonder handmatige override, zonder per post verstuurde bevestiging van statuswijzigingen en zonder alternatief indieningspad—wat vermijdbare niet-naleving garandeerde. 77. De supportcommunicatie van Kroll verergerde deze tekortkomingen—door standaard "probeer opnieuw"- en "opgelost"-berichten uit te geven, eisers door te verwijzen naar andere inboxen en geen duurzame oplossing te bieden—terwijl de deadlines voor schrapping en belastingformulieren naderden. 78. Kroll gaf een onjuiste voorstelling van zaken door te stellen dat gevoelige PII niet betrokken was en erkende later geboortedata in "ongestructureerde data" in een andere cryptoboedel (BlockFi), waardoor de waakzaamheid afnam en het succes van phishing toenam. 79. Als direct en voorzienbaar gevolg van de nalatige kennisgeving en vorderingsverwerking van Kroll, hebben Eiser en de groepsleden de vereisten voor verificatie en belastingformulieren gemist of niet kunnen voltooien die zij anders wel zouden hebben voldaan, hebben zij phishingverliezen geleden en schade door tijdswaarde en administratieve schade opgelopen. 80. Eiser en de Groepen vorderen schadevergoeding voor deze schade en een verklaring dat de kennisgevings-/verwerkingspraktijken van Kroll na het datalek onredelijk en onrechtmatig waren onder de omstandigheden. 81. Eiser en de Groepen vorderen verder een rechterlijk bevel dat meerkanaalskennisgeving vereist (e-mail en eersteklas post met getypte URL's/unieke codes), per post verstuurde bevestigingen voor elke statuswijziging die rechten beïnvloedt, gedefinieerde herstelperiodes vóór schrapping, en een handmatig/alternatief kanaal voor verificatie en indiening van belastingformulieren. Kroll blijft de op schuldeisers gerichte communicatie en administratie met betrekking tot deze boedels beheren, dus het risico op toekomstige schade is voortdurend aanwezig zonder door de rechtbank bevolen waarborgen.

GROND VIII

Nalatige Onjuiste Voorstelling van Zaken (verklaringen over het proces na het datalek)

82. Kroll heeft in communicatie na het datalek verklaard dat verificatiefouten "opgelost" waren, dat eisers "opnieuw moesten proberen", of dat de status "Geverifieerd" was, terwijl het systeem bleef terugkeren naar In de wacht/Niet-geverifieerd en de indiening van belastingformulieren blokkeerde. De rol van Kroll als door de rechtbank aangestelde vorderings-/kennisgevingsagent en Administratief Adviseur plaatste het in een positie van unieke en vertrouwde toegang tot schuldeisersinformatie en procescontrole, waardoor een bijzondere relatie ontstond die voldoende is om aansprakelijkheid voor nalatige onjuiste voorstelling van zaken te ondersteunen.

83. Kroll verstreekte deze informatie in de loop van haar professionele administratieve taken en heeft daarbij niet de redelijke zorg betracht. Eiser en de groepsleden hebben hier gerechtvaardigd op vertrouwd door door te gaan met dezelfde defecte workflow en escalatiealternatieven achterwege te laten, wat leidde tot gemiste deadlines, verliezen van tijdswaarde en schrapping.

84. Eiser vordert schadevergoeding die direct is veroorzaakt door dit vertrouwen.

GROND IX

Onrechtvaardige Verrijking (subsidiar)

85. Kroll ontving een aanzienlijke vergoeding voor haar diensten als kennisgevings-/vorderingsagent en Administratief Adviseur in de cryptoboedels, terwijl het de kosten en risico's van haar gebrekkige beveiliging en administratie na het datalek afwentelde op de eisers.

86. Het zou onbillijk zijn voor Kroll om die voordelen te behouden zonder de verliezen die het heeft

veroorzaakt te vergoeden en zonder herstelmaatregelen te financieren (inclusief monitoring, beveiligingsverbeteringen, hernieuwde kennisgeving en heropende indieningsperiodes).

87. Eiser voert onrechtvaardige verrijking subsidiair aan ten opzichte van zijn contract- en onrechtmatige daad-vorderingen voor zover de Rechtbank oordeelt dat er geen afdwingbaar contract is dat de plichten van Kroll jegens eisers regelt.

88. Eiser en de Groepen vorderen restitutie en afdracht van onrechtmatig verkregen voordelen en verrekening van vergoedingen in verhouding tot de veroorzaakte schade.

GROND X

Declaratoire en Injunctieve Vordering (28 U.S.C. §§ 2201-02)

89. Er bestaat een daadwerkelijk, berechtbaar geschil met betrekking tot de voortdurende verplichtingen van Kroll om eisersgegevens te beveiligen, adequate kennisgeving te geven van stappen die rechten beïnvloeden, en een functioneel verificatie-/belastingformulierproces te exploiteren dat conforme eisers niet willekeurig blokkeert.

90. Eiser vordert een verklaring dat de kennisgeving uitsluitend per e-mail en het afhankelijke portaal van Kroll na het datalek onredelijk waren onder de omstandigheden en dat Kroll processen moet gebruiken die redelijkerwijs berekend zijn om eisers in de toekomst te bereiken en te beschermen.

91. Eiser vordert ook een permanent rechterlijk bevel dat Kroll verplicht om, voor niet minder dan drie (3) jaar, het volgende te implementeren: (a) meerkanaalskennisgeving (e-mail en First-Class Mail) voor elke deadline die rechten beïnvloedt, met getypte URL's/unique toegangscode's en geen aanklikbare links; (b) per post verstuurde bevestigingen van elke verificatiestatuswijziging en een minimale herstelperiode van 30 dagen vóór schrapping of verbeurdverklaring; (c) versterking van wijzigingscontroles: eenmalige codes per post naar het bestaande postadres sturen voordat een e-mail-/telefoonwijziging van kracht wordt; (d) een afkoelingsperiode van 14 dagen voor wijzigingen van contactmethoden, tenzij geverifieerd door een per post verstuurde code; (e) handmatige beoordeling van overschakelingen naar recent aangemaakte ProtonMail- of andere hoogrisicodomeinen; (f) een handmatige/alternatieve methode om de verificatie te voltooiën en W-9/W-8BEN in te dienen die niet afhankelijk is van portaalvlaggen, met een gepubliceerde escalatie-SLA (escalatie binnen 5 werkdagen; oplossing binnen 10 werkdagen); (g) onveranderlijke auditlogs van statuswijzigingen en een menselijke beoordelings-override; (h) industriestandaard controles voor bezorgbaarheid en anti-spoofing (toegeweide domeinen, DMARC/SPF/DKIM-handhaving, discipline in link-tracking, het neerhalen van look-alike-domeinen gekoppeld aan FTX/Kroll/vorderingen-sleutelwoorden); (i) onafhankelijke jaarlijkse audits van beveiliging, bezorgbaarheid en portaalworkflow met rapporten beschikbaar voor de Rechtbank; en (j) gefinancierde krediet-/ID- en crypto-accountmonitoring en een vergoedingsprogramma voor phishingverlies voor getroffen eisers. 92. De gevraagde voorziening zal toekomstige schade voorkomen die met schadevergoeding alleen niet kan worden verholpen, zal een eerlijke toegang tot uitkeringen garanderen en zal de praktijken van Kroll afstemmen op de voorzienbare risico's die uniek zijn voor cryptoschuldeisers. 93. Eiser en de Groepen hebben geen adequaat rechtsmiddel voor de toekomstige schade die door de gevraagde rechterlijke bevelen wordt aangepakt; monetaire vergoeding kan geen tijdige, veilige en effectieve administratie van lopende verplichtingen van eisers garanderen. 94. De belangenafweging en het algemeen belang pleiten voor een rechterlijk bevel omdat het de rechten van duizenden eisers beschermt om gehoord te worden en uitkeringen te ontvangen zonder onnodig risico op fraude of schrapping veroorzaakt door defecte processen. 95. Eiser en de Groepen vorderen ook hun redelijke advocaatkosten en -kosten voor zover wettelijk toegestaan, inclusief onder de doctrines van het gemeenschappelijk fonds/gemeenschappelijk voordeel en de billijkheidsbevoegdheden van de Rechtbank.

ARBITRAGE-/AFSTANDSVERKLARING VAN GROEPSVORDERING 96. Het FTX-portaal is niet de "Site" van Kroll zoals gedefinieerd in de Gebruiksvoorwaarden van Kroll. Eiser heeft in het FTX-portaal niet ingestemd met enige Voorwaarden van Kroll. Het FTX-portaal bevatte alleen een toestemming voor gegevensverwerking van FTX; het toonde geen Voorwaarden van Kroll, geen arbitrage en geen afstandsverklaring van groepsvordering. Voor zover Kroll verwijst naar een afzonderlijke doorklik op haar EPOC of Kroll-site, is de clausule beperkt en electief, en is deze alleen van toepassing op geschillen "die voortvloeien uit of verband houden met deze Voorwaarden of onze Site", en er is geen delegatieclausule—dus deze Rechtbank beslist over de vatbaarheid voor arbitrage. De vorderingen van Eiser vloeien voort uit de door de rechtbank aangestelde administratie- en gegevensbeveiligingsplichten van Kroll (M365-datalek; kennisgevingskanalen na het datalek; gebrek aan een niet-afhankelijk pad voor belastingformulieren), die

onafhankelijk van enig websitegebruik bestaan en buiten elke site-beperkte clausule vallen. Subsidiair is het afdwingen van arbitrage/afstandsverklaring van groepsvordering als voorwaarde voor het indienen van een federaal Formulier 410 procedureel onbillijk; en onder het openbare beleid van New York kan grove nalatigheid niet contractueel worden geëxcuseerd. De "individuele basis"-taal van de Voorwaarden is beperkt tot arbitrage; er is geen op zichzelf staande afstandsverklaring van groepsvordering in de rechtbank. De uitzondering voor het Kroll Beveiligingsincident in het Plan bevestigt dat dit onafhankelijke vorderingen uit onrechtmatige daad van derden zijn die bedoeld zijn om 'in een andere procedure' te worden voortgezet, wat elke theorie van de niet-ondertekenaar ondermijnt.

PETITUM

WESHALVE, Eiser, individueel en namens de andere leden van de in deze Dagvaarding voorgestelde Groepen, de Rechtbank respectvol verzoekt om een vonnis in hun voordeel en tegen Gedaagde te wijzen, als volgt:

A. Voor een Bevel dat deze vordering certificeert als een groepsvordering en Eiser en zijn raadsman aanstelt om de Groepen te vertegenwoordigen;

B. Voor een billijkheidsmaatregel die restitutie en afdracht van de onrechtmatig behouden inkomsten als gevolg van het onrechtmatige gedrag van Gedaagde vereist;

C. Voor een toekenning van daadwerkelijke schadevergoeding, compensatoire schadevergoeding, wettelijke schadevergoeding en wettelijke boetes, tot een nader te bepalen bedrag, zoals wettelijk toegestaan;

D. Voor een toekenning van punitieve schadevergoeding, zoals wettelijk toegestaan;

E. Rechtsmiddelen onder de Texas DTPA: economische schade, drievoudige schadevergoeding voor willens en wetens/opzettelijke schendingen, en redelijke en noodzakelijke advocaatkosten (DTPA § 17.50(d));

F. New York GBL §§ 349/350 (subsidiair): wettelijke schadevergoeding en advocaatkosten;

G. Voor een toekenning van advocaatkosten en -kosten, en andere uitgaven, inclusief honoraria van deskundigen;

H. Wettelijke rente voor en na het vonnis over alle toegekende bedragen; en

I. Zodanige andere en verdere voorzieningen als deze rechtbank rechtvaardig en passend acht.

Datum: 19 augustus 2025

Hoogachtend,

HALL ATTORNEYS, P.C.

Door: /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

ADVOCaat VOOR EISER EN VERONDERSTELDE GROEPEN

