

& IMPORTANT DISCLAIMER

IMPORTANT DISCLAIMER

This document was translated from English to Italian 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 Italian, do not make omissions, do not fabricate falsehoods."

TRANSLATED DOCUMENT

**TRIBUNALE DISTRETTUALE DEGLI STATI UNITI PER IL DISTRETTO OCCIDENTALE DEL
TEXAS DIVISIONE DI AUSTIN**

JACOB KEVYN REPKO, in proprio e per conto di tutti gli altri soggetti in situazioni analoghe,

Attore,

contro

KROLL RESTRUCTURING

ADMINISTRATION LLC (già Prime Clerk LLC),

Convenuto.

)

) N. di Causa: 1:25-cv-01319

)

)

) ATTO DI CITAZIONE PER AZIONE COLLETTIVA

)

)

)

) RICHIESTA DI PROCESSO CON GIURIA

)

)

)

ATTO DI CITAZIONE PER AZIONE COLLETTIVA

L'Attore Jacob Kevyn Repko ("Attore"), in proprio e per conto di tutti gli altri soggetti in situazioni analoghe, per il tramite dei sottoscritti difensori, con il presente atto espone quanto segue nei confronti del Convenuto Kroll Restructuring Administration LLC (già Prime Clerk LLC) ("Kroll" o "Convenuto"). Sulla base di conoscenza personale, nonché di informazioni e convinzioni, l'Attore espone specificamente quanto segue:
NATURA DELL'AZIONE

1. La presente è un'azione collettiva per violazione di dati e negligente amministrazione derivante dall'incidente di sicurezza di Kroll del 19 agosto 2023 e dalla sua successiva incapacità di amministrare con ragionevole cura i processi e le notifiche rivolte ai creditori in tre grandi procedure fallimentari di società di criptovalute: FTX, BlockFi e Genesis.

2. La violazione di Kroll ha esposto (tra gli altri campi) nomi, indirizzi, indirizzi e-mail, numeri di telefono, identificativi/importi dei crediti e copie dei moduli di insinuazione al passivo — precisamente i metadati che i criminali sfruttano per colpire le vittime nel settore delle criptovalute con attacchi di phishing e "wrench" (minacce fisiche).

3. Dopo la violazione, Kroll ha persistito nell'inviare notifiche critiche esclusivamente via e-mail (incluse la 130^a Obiezione Omnibus di FTX, la verifica dei crediti e le scadenze per i moduli fiscali), nonostante (a) diffuse imitazioni a scopo di phishing che hanno indotto molti creditori a evitare di aprire le e-mail di "Kroll" e (b) la dimostrata capacità di Kroll di inviare lettere tramite posta prioritaria USPS quando lo riteneva opportuno — ad esempio, nel caso Genesis, dove Kroll ha spedito le notifiche della violazione tramite Posta Prioritaria.

4. I tribunali fallimentari federali avevano secretato le Informazioni di Identificazione Personale (PII) dei creditori proprio per prevenire crimini mirati al settore delle criptovalute, citando i danni reali osservati nella procedura fallimentare di Celsius (attacchi di phishing e "wrench"). Il fascicolo processuale di Genesis documenta queste preoccupazioni in ordinanze che secretano le informazioni dei clienti.

5. L'Attore Jacob Kevyn Repko (Dripping Springs, Texas) ha presentato un'insinuazione al passivo come cliente di FTX, ricevendo poi la notifica della violazione da parte di Kroll il 24 agosto 2023. Le sue PII e i dati del suo credito erano tra i dati compromessi.

6. Nei mesi successivi, il Portale per le Insinuazioni dei Clienti FTX (il "Portale FTX") ha ripetutamente manifestato malfunzionamenti: il KYC dell'Attore risultava "Verificato", per poi tornare a "In Sospeso/Non Verificato", impedendogli di caricare il modulo IRS (W-9) necessario per ricevere le distribuzioni, nonostante decine di e-mail di supporto.

7. Poiché il Portale FTX consente il caricamento dei moduli fiscali solo dopo la "Verifica KYC", l'Attore non può completare i prerequisiti finali; secondo il piano omologato e le comunicazioni del trust, i crediti possono essere espunti o le distribuzioni possono essere perse se i moduli fiscali non vengono caricati tempestivamente.

8. L'Attore ha anche subito una perdita diretta a causa di phishing a seguito della violazione: ha trasferito 1.9 ETH da un conto di exchange al suo hot wallet alle 12:43 del 3 luglio 2025, e l'importo è stato deviato tramite un bot di transazione automatizzato, comunemente usato per intercettare trasferimenti in sospeso, verso un wallet non controllato dall'Attore, in linea con l'avvertimento di Kroll stessa secondo cui gli aggressori avrebbero usato i dati trapelati per attacchi di phishing a conti di criptovalute.

PARTI

9. L'Attore Jacob Repko è una persona fisica domiciliata nella Contea di Hays, Texas. È un cliente-creditore di FTX con un credito ammesso di \$87.487,93.

10. Il Convenuto Kroll Restructuring Administration LLC è una LLC del Delaware con significative operazioni a livello nazionale, inclusi uffici in Texas.

11. Sulla base di informazioni e convinzioni, l'Attore cita in giudizio anche i Soggetti Ignoti 1-5, entità non identificate al momento, diverse da Kroll, che hanno partecipato, se del caso, alla verifica dei richiedenti o alla ricezione dei moduli fiscali (inclusi fornitori terzi di servizi KYC). Nella misura in cui un'entità non-Kroll abbia controllato gli indicatori di stato KYC o l'accesso al caricamento dei moduli W-9/W-8 all'interno del Portale FTX, l'Attore formula tali accuse in via alternativa e modificherà l'atto sostituendo i nomi reali una volta identificati. Se Kroll designerà una terza parte responsabile, l'Attore la chiamerà tempestivamente in causa secondo le norme sulla responsabilità proporzionale del Texas.

GIURISDIZIONE E FORO COMPETENTE

12. Questo Tribunale ha giurisdizione per materia ai sensi del 28 U.S.C. § 1332(d) (CAFA): le classi proposte superano i 100 membri; il valore aggregato della controversia supera i \$5.000.000; esiste una diversità minima (attore del Texas contro convenuto del Delaware/New York con membri della classe a livello nazionale/internazionale).

13. Questo Tribunale ha giurisdizione personale su Kroll perché Kroll mantiene uffici ad Austin, Dallas e Houston, dirige intenzionalmente attività di amministrazione/notifica e comunicazioni con i richiedenti verso il Texas, e ha commesso atti che hanno causato un danno a un residente del Texas in questo Distretto. Le pretese dell'Attore derivano da o sono correlate a tale condotta nel foro, e l'esercizio della giurisdizione è conforme al giusto processo.

14. Il foro è competente ai sensi del 28 U.S.C. § 1391(b) perché una parte sostanziale degli eventi e dei danni si è verificata in questo Distretto: l'Attore risiede qui, ha ricevuto le notifiche di Kroll qui, ha

utilizzato il Portale per le Insinuazioni dei Clienti FTX (claims.ftx.com) e poi l'Insinuazione al Passivo Elettronica ("EPOC") di Kroll qui, e ha subito una perdita per phishing qui.

15. Al momento, l'Attore non avanza pretese contro i Debitori, o qualsiasi parte liberata dal piano, e non chiede un provvedimento che richieda l'interpretazione, la modifica o l'esecuzione del Piano o dell'Ordinanza di Omologazione. Si tratta di pretese indipendenti per illecito/contratto contro Kroll, soggetto non debitore. La presente azione non è un procedimento "core"; l'Attore richiede un processo con giuria e non acconsente alla giurisdizione del tribunale fallimentare.

DEFINIZIONI

16. "Portale per le Insinuazioni dei Clienti FTX" o "Portale FTX" indica il portale all'indirizzo claims.ftx.com gestito per i Debitori/FTX Recovery Trust (con fornitori) per gestire le procedure KYC/AML e la revisione dei conti. "Sito Kroll" indica il sito web di Kroll, inclusa l'interfaccia EPOC su restructuring.ra.kroll.com, che ha ricevuto le presentazioni del Modulo fallimentare 410 e ha mantenuto il registro pubblico delle insinuazioni. Laddove il controllo non sia chiaro, l'Attore formula le accuse in via alternativa contro i Convenuti Ignoti da sostituire una volta identificati.

ESPOSIZIONE DEI FATTI

A. La Violazione di Kroll ha Coinvolto FTX, Genesis e BlockFi

17. Intorno al 19 agosto 2023, un aggressore ha effettuato un'operazione di SIM-swapping sul telefono di un dipendente di Kroll, accedendo ai file cloud di Kroll contenenti i dati dei richiedenti per ciascuna massa fallimentare. Informazioni indipendenti sulla minaccia confermano che i campi compromessi sono stati successivamente monetizzati e resi operativi da attori fraudolenti che hanno preso di mira i richiedenti di FTX e le transazioni sul mercato secondario.

18. Il documento depositato da Kroll nel caso Genesis ammette che i dati interessati includevano nomi, numeri di telefono, indirizzi, numeri/importi dei crediti, saldi di wallet/cryptovalute e copie delle insinuazioni al passivo.

19. La notifica di BlockFi dettaglia ulteriormente che data di nascita, indirizzo postale e numeri di patente di guida erano coinvolti e riferisce della tardiva identificazione da parte di Kroll di una grande quantità di "File Non Strutturati".

B. I Tribunali hanno Secretato le PII dei Creditori perché i Creditori di Criptovalute Affrontano Vettori di Attacco Unici

20. Nel caso Genesis, il tribunale ha emesso ordinanze di secretazione per proteggere i nomi/informazioni di contatto dei creditori, facendo riferimento all'esperienza di Celsius dove attacchi di phishing e "wrench" sono seguiti a divulgazioni pubbliche.

C. Kroll Sapeva che l'E-mail non era Sicura ma non ha Utilizzato la Posta per le Notifiche Critiche

21. Sulla base di informazioni e convinzioni, Kroll ha avvertito pubblicamente i creditori di Genesis riguardo al phishing e ha inviato notifiche della violazione tramite Posta Prioritaria per garantirne la consegna.

22. Tuttavia, nel caso FTX, per notifiche di uguale (o maggiore) importanza — incluse le scadenze della 130ª Obiezione Omnibus (ad es., iniziare il KYC entro il 1° marzo 2025; completarlo entro il 1° giugno 2025) e la scadenza per i moduli fiscali — Kroll si è affidata principalmente all'e-mail solo pochi mesi dopo la propria violazione che ha scatenato il phishing, sapendo che molti destinatari non avrebbero aperto le e-mail di "Kroll" per paura di truffe o le avrebbero trovate nella posta indesiderata/spam. Informazioni pubbliche sulla minaccia mostrano acquisizioni di account tramite phishing in cui i perpetratori hanno cambiato le e-mail dei richiedenti con nuovi indirizzi ProtonMail e hanno superato rapidamente le sfide 2FA — precisamente l'attacco che l'approccio basato solo sull'e-mail di Kroll non ha mitigato.

23. Il Portale FTX consente il caricamento dei moduli W-9/W-8BEN solo dopo la verifica KYC. Quando il portale riporta erroneamente un utente a "In Sospeso/Non Verificato", il passaggio del modulo fiscale diventa impossibile — rischiando l'espunzione del credito o la perdita delle distribuzioni secondo i processi del piano comunicati ai creditori. In un ambiente in cui i richiedenti sono stati indotti a evitare le e-mail di "Kroll" a causa di imitazioni attive, un passaggio per il modulo fiscale accessibile solo online e condizionato, senza un'alternativa via Posta Prioritaria, non era ragionevolmente calcolato per informare o consentire il completamento.

24. L'ordinanza di omologazione di FTX prevede espressamente che Kroll non sia liberata o esonerata

da responsabilità per le pretese relative all'"Incidente di Sicurezza" e che i danni ai clienti recuperabili in un altro procedimento non siano limitati dalle distribuzioni del piano. L'Attore chiede rispettosamente che si prenda atto giudizialmente di tale estratto dell'ordinanza di omologazione ai sensi della Fed. R. Evid. 201.

25. Oltre ad essere stata incaricata dal tribunale fallimentare ai sensi del §156(c) per le notifiche, Kroll è stata ingaggiata come Consulente Amministrativo per svolgere servizi di amministrazione fallimentare secondo i suoi documenti di incarico e l'ordinanza di nomina del Tribunale. Questi doveri rivolti ai creditori (sollecitazione/votazione/tabulazione e gestione delle comunicazioni con i richiedenti) supportano gli obblighi di amministrazione qui contestati.

D. L'Esperienza dell'Attore

26. L'Attore ha presentato la sua insinuazione al passivo come cliente utilizzando il Portale FTX e, quando richiesto, depositando il Modulo fallimentare 410 tramite l'EPOC di Kroll.

27. Ha ricevuto la notifica della violazione da parte di Kroll che confermava l'esposizione del suo nome, indirizzo, e-mail e saldo del conto e avvertiva di phishing mirato ai beni in criptovaluta.

28. Dopo aver lottato con blocchi del portale e ritardi, il KYC dell'Attore è stato verificato intorno al 3 novembre 2023, ma il portale è successivamente tornato a "In Sospeso", bloccando il caricamento del modulo IRS; innumerevoli e-mail a Kroll sono rimaste senza risposta.

29. Dopo la violazione, l'Attore è stato vittima di phishing: 1.9 ETH sono stati prosciugati pochi minuti dopo essere arrivati nel suo hot wallet (arrivo alle 12:43; uscita alle 12:49 verso l'indirizzo dell'aggressore).

30. L'Attore detiene un credito ammesso in FTX di \$87.487,93 e ora rischia la perdita di parte o di tutto il valore della distribuzione perché non può soddisfare i prerequisiti del piano a causa di malfunzionamenti del portale e mancate notifiche.

31. L'Attore ha subito danni concreti, tra cui: (a) uso improprio effettivo — furto di 1.9 ETH pochi minuti dopo l'arrivo nel suo wallet il 3 luglio 2025; (b) danni legati al valore temporale e alle distribuzioni a causa del blocco della verifica/presentazione del modulo fiscale; (c) costi di mitigazione sostenuti di tasca propria; (d) perdita di privacy/controllo delle PII; e (e) rischio sostanziale di uso improprio futuro dati i modelli di attacco mirati al settore delle criptovalute qui documentati.

E. Uso Improprio Sistemático dei Dati dei Richiedenti Trapelati

32. La prevedibilità non è un'astrazione: gli investigatori hanno tracciato frodi per 5,6 milioni di dollari che sfruttavano i dati delle insinuazioni di FTX, incluse vendite di set di dati dei richiedenti sul dark web e modelli di cambio e-mail/bypass 2FA — esattamente i danni che i tribunali cercavano di prevenire secretando le PII dei creditori di criptovalute. La comunicazione contraria di Kroll, secondo cui nessuna PII sensibile era a rischio, ha indotto in errore i consumatori sulla necessità di trattare ogni e-mail di "Kroll" come sospetta e di richiedere un supporto via posta ordinaria.

33. Informazioni indipendenti sulla minaccia corroborano che i dati dei richiedenti di FTX sono stati attivamente utilizzati come arma contro creditori e controparti. Tra luglio e novembre 2024, gli investigatori hanno documentato frodi per almeno 5,6 milioni di dollari legate alla negoziazione di crediti FTX, in cui un attore (o un gruppo) si è impersonato come titolare di crediti utilizzando selfie alterati con IA, nuovi account ProtonMail e documenti di identificazione falsificati.

34. La tecnica dell'attore includeva: (a) indirizzi ProtonMail creati di recente sostituiti all'e-mail originale del richiedente; (b) inserimento rapido di codici 2FA, suggerendo l'acquisizione dell'account; e (c) riciclaggio tramite indirizzi di deposito di Gate.io, CoinEx e Binance. Questi modelli sono coerenti con la compromissione delle credenziali tramite phishing a seguito dell'incidente di Kroll.

35. La stessa ricerca mostra dati dei crediti FTX pubblicizzati su forum del dark web, inclusi nomi, telefoni, e-mail, dettagli di wallet/transazioni e altri dati legati ai crediti — gli stessi campi che Kroll ha ammesso essere stati compromessi (nomi, e-mail, numeri di telefono, indirizzi postali, identificativi e saldi dei conti, e in alcuni casi date di nascita).

36. Gli investigatori hanno anche osservato cambi di e-mail verso account ProtonMail creati dopo la chiusura per crediti originariamente aperti con e-mail diverse, indicando l'acquisizione e l'impersonificazione degli account dei richiedenti.

37. Il rapporto documenta i percorsi sulla blockchain dai wallet degli impersonatori agli indirizzi di deposito di CoinEx e identifica un wallet intermediario associato ad attività di transazione automatizzata; nota interazioni con exchange statunitensi (Coinbase e Kraken) che possono essere citati in giudizio per il KYC. Ciò evidenzia un modello di frode coeso e ripetibile che sfrutta le PII dei richiedenti e le debolezze

del flusso di lavoro.

38. Il rapporto nota inoltre un errore "Orbeon Forms – Page Not Found" emerso durante una verifica di due diligence del Portale FTX — coerente con un flusso di lavoro fragile per i richiedenti e stati di errore che gli attori malintenzionati possono imitare, amplificando la confusione in un ambiente ad alto rischio di phishing.

F. Dichiarazioni False e Omissioni Post-Violazione

39. Kroll, pubblicamente e nelle comunicazioni ai richiedenti, ha minimizzato la portata della violazione — affermando inizialmente che nessuna PII sensibile era stata compromessa. In altre procedure che amministrava (ad es., BlockFi), Kroll ha successivamente rivelato che le date di nascita erano contenute in "dati non strutturati", contraddicendo le sue dichiarazioni iniziali. Kroll ha altresì detto ai richiedenti di FTX che potevano continuare a interagire con i flussi di lavoro basati su e-mail e non ha avvertito che attori malintenzionati stavano impersonando Kroll e cambiando gli indirizzi e-mail dei richiedenti con account ProtonMail appena creati per eludere la 2FA — modelli confermati da informazioni indipendenti sulla minaccia. Queste dichiarazioni e omissioni erano materiali, rivolte ai consumatori e fuorvianti, e hanno indotto i richiedenti ragionevoli a sottovalutare il rischio, a continuare a utilizzare canali esclusivamente via e-mail e a ritardare rimedi più forti, contribuendo a perdite per phishing, danni legati al valore temporale e scadenze mancate con conseguente espunzione dei crediti.

MOTIVI RELATIVI ALL'AZIONE COLLETTIVA

40. Classe Globale dei Creditori di Criptovalute: Tutte le persone in tutto il mondo le cui PII o dati di credito forniti a Kroll per le procedure fallimentari di FTX, BlockFi o Genesis sono stati consultati, esfiltrati o ragionevolmente a rischio nell'incidente di Kroll dell'agosto 2023. L'appartenenza alla classe è accertabile dagli elenchi di notifica di Kroll, dai registri EPOC e dai registri dei crediti delle masse fallimentari che identificano gli individui i cui dati Kroll ammette essere stati consultati o ragionevolmente a rischio nell'incidente.

41. Sottoclassi per Massa Fallimentare: (a) Sottoclasse FTX; (b) Sottoclasse BlockFi; e (c) Sottoclasse Genesis.

L'Attore aggiungerà rappresentanti nominati per le sottoclassi BlockFi e Genesis al momento della certificazione della classe o prima.

42. Sottoclassi per Danno (trasversali alle masse fallimentari): (i) Sottoclasse phishing/perdita di criptovalute; (ii) Sottoclasse portale/verifica/modulo fiscale (perdita per espunzione, perdita di valore temporale e danno amministrativo);

(iii) Sottoclasse per danno standard da violazione di dati (violazione della privacy, costi di mitigazione).

43. I requisiti di numerosità, comunanza, tipicità e adeguatezza sono soddisfatti: le questioni comuni includono se Kroll avesse e abbia violato i doveri di sicurezza dei dati, adeguatezza della notifica e amministrazione del processo di insinuazione; se la notifica esclusivamente via e-mail fosse ragionevole dopo la violazione; e se sia giustificato un provvedimento ingiuntivo.

LEGGE APPLICABILE

44. Gli standard che regolano la condotta sono disciplinati dalla legge di New York (Kroll ha sede e ha agito da NY), o in alternativa dalla legge del Texas per i residenti e i danni in Texas. Le pretese si basano su doveri/atti comuni a tutti i membri della classe. Le questioni di arbitrabilità sono regolate dal FAA; la politica pubblica di New York vieta l'esenzione contrattuale dalla responsabilità per colpa grave.

TITOLI DELLA DOMANDA

TITOLO I

Negligenza (Colpa) (legge di New York; in alternativa legge del Texas)

45. Kroll aveva un dovere nei confronti dell'Attore e delle Classi (FTX, BlockFi e Genesis) di esercitare una ragionevole cura nella raccolta, conservazione, trasmissione e amministrazione delle PII e dei dati dei crediti dei richiedenti; di progettare, gestire e supportare un flusso di lavoro funzionale per la verifica/modulo fiscale; e — specialmente dopo l'incidente del 19 agosto 2023 — di fornire notifiche ragionevolmente calcolate, in tutte le circostanze, per informare i richiedenti delle scadenze e dei passaggi che incidono sui loro diritti e per mitigare i rischi prevedibili di phishing e di recapitabilità.

46. Tali doveri derivavano da (a) i ruoli di Kroll come agente per le notifiche/insinuazioni nominato dal tribunale e Consulente Amministrativo; (b) ordinanze del tribunale che secretavano le PII dei creditori di

criptovalute a causa di noti rischi di phishing e sicurezza fisica; (c) la conoscenza e gli avvertimenti di Kroll stessa che le e-mail dei richiedenti esposte sarebbero state bersaglio di phishing; e (d) il controllo di Kroll sulle comunicazioni con i richiedenti e sulla ricezione tramite EPOC; nella misura in cui un'entità non-Kroll abbia controllato gli indicatori di stato KYC e l'accesso al modulo fiscale all'interno del Portale FTX, l'Attore formula tali accuse in via alternativa contro i Convenuti Ignoti da sostituire una volta identificati. Questi doveri sono indipendenti da qualsiasi contratto e riconosciuti dalla legge di New York e del Texas laddove la condotta di una parte crei o aumenti un rischio prevedibile di furto di identità/beni per una classe nota e finita (richiedenti di criptovalute con PII segretate), e laddove le scelte di notifica e processo post-violazione siano regolate da principi di giusto processo (ad es., Mullane; Jones v. Flowers) e dalle ordinanze del tribunale fallimentare in materia di privacy/notifica.

47. Kroll ha violato i suoi doveri, tra l'altro: (i) permettendo la compromissione, tramite SIM-swapping, dei repository cloud contenenti i dati dei richiedenti; (ii) non identificando prontamente e completamente tutti gli archivi di dati interessati; (iii) persistendo — dopo la violazione — nella notifica esclusivamente via e-mail per comunicazioni che incidono sui diritti, anche se molti richiedenti non potevano distinguere le e-mail legittime di Kroll dal phishing e anche se Kroll aveva la capacità e il precedente per inviare Posta Prioritaria; (iv) consentendo un flusso di lavoro per la distribuzione in cui il caricamento dei moduli W-9/W-8BEN era bloccato a meno che il KYC non risultasse "Verificato" nel Portale FTX, senza fornire un percorso di presentazione manuale/alternativo tramite l'EPOC di Kroll o via posta/e-mail; (v) non fornendo alcun percorso di presentazione manuale/alternativo o conferme postali per i cambi di stato; (vi) fornendo un supporto circolare, ritardato o inefficace che ha prolungato e aggravato il danno; (vii) non implementando, dopo la violazione, un rafforzamento del controllo delle modifiche (codice spedito al vecchio indirizzo per qualsiasi cambio di e-mail/telefono; periodi di attesa forzati; revisione manuale delle modifiche verso account ProtonMail creati dopo novembre 2022) nonostante le prove di modelli di acquisizione di e-mail contro i richiedenti; e (viii) non implementando il monitoraggio del dark web e la rimozione di domini simili basati su parole chiave relative a FTX/Kroll dopo che sono state osservate online offerte di set di dati dei richiedenti.

48. I rischi che Kroll ha creato e non ha mitigato erano prevedibili: i tribunali federali nei casi di criptovalute avevano secretato le PII dei clienti per prevenire attacchi di phishing e "wrench"; le forze dell'ordine federali e le guide sulla sicurezza avvertono i detentori di asset digitali di mantenere private le informazioni identificative; e Kroll stessa ha detto ai richiedenti che gli aggressori avrebbero inviato e-mail convincenti per impossessarsi di account e wallet. In queste circostanze, l'uso esclusivo dell'e-mail per passaggi e scadenze critiche per i diritti non era ragionevole.

49. Gli atti e le omissioni di Kroll sono stati la causa diretta e prossima dei danni dell'Attore e dei membri della classe. Se non fosse stato per le falle di sicurezza di Kroll, la notifica esclusivamente via e-mail, il rifiuto di inviare posta ordinaria per le scadenze della 130^a Obiezione Omnibus e per la scadenza del modulo fiscale, e il portale difettoso e condizionato, l'Attore e molti membri della classe avrebbero iniziato e completato tempestivamente la verifica e presentato i moduli fiscali; non avrebbero avuto i crediti espunti o messi "in sospeso" ritardando così le distribuzioni del piano; e avrebbero evitato perdite per phishing e costi di mitigazione.

50. L'Attore e le Classi hanno subito danni, inclusi, senza limitazione: (a) perdite per phishing/criptovalute (per l'Attore 1.9 ETH prosciugati pochi minuti dopo la ricezione); (b) danni legati al valore temporale a causa di ritardi nella distribuzione causati dalla notifica esclusivamente via e-mail e dai difetti del portale; (c) espunzione/perdita del credito legata a scadenze mancate per la verifica/modulo fiscale; (d) spese vive (monitoraggio, rafforzamento di dispositivi/wallet, ottenimento di documenti) e tempo perso; e (e) diminuzione della privacy e furto continuo di identità e beni.

51. L'Attore e le Classi chiedono il risarcimento dei danni emergenti e del lucro cessante in un importo da provare in giudizio, unitamente agli interessi pre e post-sentenza.

TITOLO II

Legge del Texas sulle Pratiche Commerciali Ingannevoli a Tutela dei Consumatori (Tex. Bus. & Com. Code § 17.41 e segg.)

52. L'Attore è un consumatore ai sensi del Tex. Bus. & Com. Code §17.45(4) perché ha richiesto e utilizzato servizi — l'amministrazione delle insinuazioni di Kroll e i servizi rivolti ai creditori acquistati a beneficio dell'Attore dai Debitori FTX/FTX Recovery Trust — e tali servizi sono stati forniti all'Attore per consentirgli di far valere e ricevere distribuzioni sul suo credito.

53. Kroll ha posto in essere atti ingannevoli, tra cui: (1) rappresentare che i servizi avevano caratteristiche/benefici che non avevano — ovvero, che nessuna PII sensibile (ad es., nome completo, indirizzo postale, data di nascita, dettagli di wallet/transazioni) era stata sottratta e che i processi via e-mail erano sicuri dopo la violazione;

(2) omettere di divulgare informazioni note al momento delle transazioni (che PII sensibili erano presenti in "dati non strutturati"; che erano in atto impersonificazioni/acquisizioni tramite cambio e-mail) per indurre i richiedenti a continuare il flusso di lavoro esclusivamente via e-mail; e (3) rappresentare diritti/obblighi nell'ambito del processo di insinuazione che non avevano — implicando che la sola notifica via e-mail fosse ragionevole e sufficiente per scadenze critiche per i diritti.

54. All'indomani di un noto incidente di sicurezza e di una campagna di phishing in corso, persistere con la notifica esclusivamente via e-mail per scadenze critiche per i diritti e omettere un supporto postale e un canale di presentazione manuale dei moduli fiscali è stato un comportamento iniquo che ha approfittato in modo gravemente ingiusto della mancanza di conoscenza e dell'incapacità dei richiedenti di proteggersi.

55. Le violazioni del DTPA da parte di Kroll sono state la causa efficiente dei danni dell'Attore, inclusi (i) il furto di 1.9 ETH a seguito di phishing, (ii) danni legati al valore temporale/distribuzioni a causa del blocco della verifica e della presentazione del modulo fiscale, e (iii) costi di mitigazione e perdita di privacy/controllo delle PII.

56. Kroll ha agito consapevolmente, e per certi aspetti intenzionalmente: sapeva dalle proprie indagini in altre masse fallimentari (ad es., BlockFi) che PII sensibili esistevano in "dati non strutturati", eppure ha detto ai richiedenti il contrario e non ha adeguato di conseguenza le notifiche e i flussi di lavoro.

57. L'Attore chiede il risarcimento dei danni economici, le spese legali, i costi e il triplo del danno per violazioni consapevoli/intenzionali ai sensi del DTPA del Texas.

58. L'Attore ha inviato o sta inviando contestualmente la notifica pre-contenziosa. Nella misura in cui la notifica non fosse fattibile a causa di prescrizioni imminenti e della necessità di un provvedimento ingiuntivo, l'Attore chiede al Tribunale di sospendere la domanda basata sul DTPA per 60 giorni dalla notifica per consentire discussioni su possibili rimedi come previsto dalla legge.

TITOLO III

Atti Ingannevoli e Sleali secondo la legge di New York (in via alternativa)

59. Kroll ha posto in essere atti e pratiche ingannevoli rivolte ai consumatori, tra cui l'invio di notifiche processuali e comunicazioni ai richiedenti fuorvianti, minimizzando la violazione (affermando che non vi erano PII sensibili), omettendo di divulgare fatti materiali (PII presenti nei file e in "dati non strutturati"; impersonificazione attiva), e incoraggiando la continuazione delle comunicazioni esclusivamente via e-mail in un ambiente di phishing attivo. Questi atti erano fuorvianti in modo materiale e hanno danneggiato l'Attore. L'Attore chiede il risarcimento dei danni effettivi, danni statutari, spese legali ragionevoli e un provvedimento ingiuntivo ai sensi delle sezioni 349(h) e 350-e della New York General Business Law.

TITOLO IV

Colpa Grave

60. La condotta di Kroll è stata più di una semplice negligenza. Sapendo che le PII dei richiedenti erano state esposte, e sapendo che i richiedenti erano attivamente bersaglio di phishing, Kroll ha consapevolmente persistito in messaggi esclusivamente via e-mail, pieni di link e facilmente imitabili per scadenze che incidevano sui diritti; si è rifiutata di passare alla posta ordinaria su larga scala anche se ne aveva la capacità e aveva usato la posta per altre comunicazioni critiche; e ha continuato a condizionare la presentazione dei moduli fiscali a un portale di insinuazione inaffidabile che riportava ripetutamente gli utenti avanti e indietro tra "Verificato" e "In Sospeso" senza spiegazioni — anche dopo che informazioni di terze parti avevano documentato impersonificazioni continue, acquisizioni tramite cambio e-mail e percorsi di riciclaggio utilizzando i dati dei richiedenti.

61. La mancata implementazione da parte di Kroll di ovvie misure di salvaguardia — Posta Prioritaria per notifiche critiche per i diritti, conferme postali dei cambi di stato, un percorso manuale non condizionato per i moduli fiscali, rafforzamento del controllo delle modifiche (codici spediti all'indirizzo esistente; periodi di attesa; revisione manuale dei passaggi a account ProtonMail creati di recente) e monitoraggio del dark web — è stata una deviazione estrema dalla normale diligenza di fronte a un'alta probabilità di grave danno per una popolazione le cui PII erano state secrete proprio per evitare phishing e attacchi fisici.

62. La condotta gravemente negligente di Kroll è stata un fattore sostanziale nel causare i danni dell'Attore e delle Classi e giustifica la concessione di danni punitivi per punire e scoraggiare simili

comportamenti.

63. L'Attore e le Classi chiedono danni punitivi in un importo sufficiente a riflettere la riprovevolezza della condotta di Kroll e a scoraggiare future violazioni.

TITOLO V

Inadempimento di Contratto Implicito (Privacy e Amministrazione delle Insinuazioni)

64. Sollecitando e accettando le PII e le insinuazioni al passivo dell'Attore e dei membri della classe e richiedendo loro di utilizzare il Portale FTX (KYC/revisione) e l'EPOC di Kroll (deposito dell'insinuazione) per partecipare al processo di insinuazione fallimentare, Kroll ha stipulato contratti impliciti per (a) salvaguardare tali informazioni con ragionevole sicurezza, (b) amministrare i passaggi di verifica e dei moduli fiscali con ragionevole cura, e (c) fornire canali ragionevolmente progettati per garantire che i richiedenti potessero completare i passaggi che incidono sui loro diritti.

65. L'Attore e i membri della classe hanno adempiuto fornendo informazioni accurate e seguendo le istruzioni di Kroll. Si aspettavano ragionevolmente che Kroll proteggesse i loro dati e fornisse un processo funzionale e sicuro per completare la verifica e caricare i moduli fiscali.

66. Kroll ha violato queste promesse implicite consentendo l'accesso non autorizzato ai dati dei richiedenti; continuando a utilizzare notifiche esclusivamente via e-mail in un noto ambiente di phishing; persistendo in un flusso di lavoro difettoso e condizionato senza un percorso alternativo; e non fornendo un'opzione di presentazione manuale non condizionata o conferme postali per i cambi di stato che incidono sui diritti.

67. Come risultato diretto e prossimo, l'Attore e i membri della classe hanno subito i danni sopra descritti, tra cui perdite per phishing, danni legati al valore temporale e alle distribuzioni, e costi vivi.

68. L'Attore e le Classi chiedono il risarcimento dei danni, la restituzione e ogni altro provvedimento appropriato per l'inadempimento del contratto implicito da parte di Kroll.

TITOLO VI

Assunzione Negligente di un Obbligo (Restatement (Second) of Torts § 324A)

69. Kroll si è impegnata a rendere servizi che sapeva essere necessari per la protezione dell'Attore e delle Classi — ovvero, salvaguardare le PII dei richiedenti e amministrare il flusso di lavoro di verifica/modulo fiscale e le notifiche che incidono sui diritti.

70. Kroll ha eseguito tale impegno in modo negligente utilizzando la notifica esclusivamente via e-mail dopo la violazione; rifiutando di inviare posta ordinaria per le scadenze della 130^a Obiezione Omnibus e per la scadenza del modulo fiscale; condizionando la presentazione del modulo fiscale a un flusso di lavoro inaffidabile e basato sullo stato; e non fornendo un percorso alternativo o conferme postali.

71. L'esecuzione negligente da parte di Kroll ha aumentato il rischio di danno per l'Attore e i membri della classe (notifiche mancate o ignorate, blocchi dovuti a cambi di stato, phishing) ed è stata un fattore sostanziale nelle perdite risultanti.

72. L'Attore e molti membri della classe hanno fatto affidamento sull'impegno di Kroll — utilizzando il Portale FTX e le comunicazioni/EPOC di Kroll come istruito e rinunciando ad altri passaggi perché Kroll era il canale esclusivo per la verifica e l'amministrazione delle insinuazioni.

73. L'Attore e le Classi hanno diritto al risarcimento dei danni causati prossimamente dall'assunzione negligente di un obbligo da parte di Kroll.

TITOLO VII

Negligenza nella Notifica e Gestione delle Insinuazioni Post-Violazione

74. Dopo l'incidente del 19 agosto 2023, Kroll aveva un dovere accresciuto di mitigare i danni prevedibili e di fornire notifiche e adeguamenti procedurali ragionevolmente calcolati per raggiungere i richiedenti e consentire il tempestivo adempimento dei passaggi che incidono sui diritti.

75. Kroll ha violato tale dovere continuando a fare affidamento sulla notifica esclusivamente via e-mail — nonostante il phishing pervasivo e il filtraggio antispam diretto a e-mail simili a quelle di Kroll — e non passando alla posta ordinaria per le comunicazioni più importanti, inclusa la 130^a Obiezione Omnibus di FTX

e le relative scadenze (da iniziare entro il 1° marzo 2025 e completare entro il 1° giugno 2025) e la scadenza del modulo fiscale. Il piano omologato non conteneva date fisse nel testo del piano; pertanto, la scelta del canale da parte di Kroll ha reso tali notifiche determinanti per l'esito. Molti richiedenti ragionevoli non hanno aperto le e-mail di Kroll perché farlo sembrava una "roulette russa" durante campagne di

phishing attive; molte notifiche sono finite nelle cartelle di posta indesiderata/spam e non sono state viste.

76. Indipendentemente, FTX gestiva un portale che bloccava la presentazione dei moduli W-9/W-8BEN a meno che il "KYC" non fosse "Verificato", eppure il sistema riportava erroneamente gli utenti verificati a "In Sospeso/Non Verificato", senza alcuna possibilità di intervento manuale, senza conferma postale dei cambi di stato e senza un percorso di presentazione alternativo — garantendo un inadempimento prevenibile.

77. Le comunicazioni di supporto di Kroll hanno aggravato queste mancanze — inviando messaggi standardizzati come "riprova" e "risolto", reindirizzando i richiedenti ad altre caselle di posta e non fornendo una soluzione duratura — mentre le scadenze per l'espunzione e i moduli fiscali si avvicinavano.

78. Kroll ha dichiarato falsamente che non erano implicate PII sensibili e ha successivamente riconosciuto la presenza di date di nascita in "dati non strutturati" in un'altra massa fallimentare di criptovalute (BlockFi), riducendo così la vigilanza e aumentando il successo del phishing.

79. Come risultato diretto e prossimo della negligenza di Kroll nella notifica e gestione delle insinuazioni, l'Attore e i membri della classe hanno mancato o non sono stati in grado di completare i requisiti di verifica e dei moduli fiscali che altrimenti avrebbero soddisfatto, hanno subito perdite per phishing e hanno subito danni legati al valore temporale e amministrativi.

80. L'Attore e le Classi chiedono il risarcimento per questi danni e una dichiarazione che le pratiche di notifica/gestione post-violazione di Kroll erano irragionevoli e illegittime date le circostanze.

81. L'Attore e le Classi chiedono inoltre un provvedimento ingiuntivo che richieda una notifica multicanale (e-mail e posta prioritaria con URL digitati/codici unici), conferme postali per qualsiasi cambio di stato che incida sui diritti, finestre di sanatoria definite prima dell'espunzione e un canale manuale/alternativo per la verifica e la presentazione dei moduli fiscali. Kroll continua ad amministrare le comunicazioni e i registri rivolti ai creditori relativi a queste masse fallimentari, quindi il rischio di danni futuri è continuo in assenza di tutele ordinate dal tribunale.

TITOLO VIII

Dichiarazione Falsa per Negligenza (dichiarazioni sul processo post-violazione)

82. Kroll, nelle comunicazioni post-violazione, ha rappresentato che gli errori di verifica erano "risolti", che i richiedenti dovevano "riprovare", o che lo stato era "Verificato", quando il sistema continuava a tornare a In Sospeso/Non Verificato e a bloccare la presentazione del modulo fiscale. Il ruolo di Kroll come agente per le insinuazioni/notifiche nominato dal tribunale e Consulente Amministrativo la poneva in una posizione di accesso unico e fiduciario alle informazioni dei creditori e al controllo del processo, creando una relazione speciale sufficiente a sostenere la responsabilità per dichiarazione falsa per negligenza.

83. Kroll ha fornito queste informazioni nel corso dei suoi doveri professionali di amministrazione e non ha esercitato una ragionevole cura. L'Attore e i membri della classe hanno fatto giustificabile affidamento continuando con lo stesso flusso di lavoro difettoso e rinunciando ad alternative di escalation, causando scadenze mancate, perdite di valore temporale ed espunzioni.

84. L'Attore chiede il risarcimento dei danni causati prossimamente da questo affidamento.

TITOLO IX

Arricchimento senza Causa (in via alternativa)

85. Kroll ha ricevuto un compenso sostanziale per aver agito come agente per le notifiche/insinuazioni e Consulente Amministrativo in tutte le masse fallimentari di criptovalute, esternalizzando i costi e i rischi della sua sicurezza carente e dell'amministrazione post-violazione sui richiedenti.

86. Sarebbe iniquo per Kroll trattenere tali benefici senza rimborsare le perdite che ha causato e senza finanziare misure correttive (incluso il monitoraggio, i miglioramenti della sicurezza, nuove notifiche e la riapertura delle finestre di presentazione).

87. L'Attore invoca l'arricchimento senza causa in alternativa alle sue pretese contrattuali e per illecito nella misura in cui il Tribunale ritenga che nessun contratto esecutivo regoli i doveri di Kroll nei confronti dei richiedenti.

88. L'Attore e le Classi chiedono la restituzione e la retrocessione dei benefici illecitamente ottenuti e compensazioni sulle commissioni commisurate ai danni causati.

TITOLO X

Provvedimento Dichiarativo e Ingiuntivo (28 U.S.C. §§ 2201-02)

89. Esiste una controversia attuale e giustiziabile riguardo agli obblighi continui di Kroll di proteggere i dati dei richiedenti, di dare adeguata notifica dei passaggi che incidono sui diritti e di gestire un processo di verifica/modulo fiscale funzionale che non blocchi arbitrariamente i richiedenti adempienti.

90. L'Attore chiede una dichiarazione che la notifica esclusivamente via e-mail e il portale condizionato post-violazione di Kroll erano irragionevoli date le circostanze e che Kroll deve impiegare processi ragionevolmente calcolati per raggiungere e proteggere i richiedenti in futuro.

91. L'Attore chiede anche un'ingiunzione permanente che richieda a Kroll, per non meno di tre (3) anni, di implementare: (a) notifica multicanale (e-mail e Posta Prioritaria) per qualsiasi scadenza che incida sui diritti, con URL digitati/codici di accesso unici e nessun link cliccabile; (b) conferme postali di qualsiasi cambio di stato di verifica e una finestra di sanatoria minima di 30 giorni prima dell'espunzione o della perdita; (c) rafforzamento del controllo delle modifiche: codici monouso spediti all'indirizzo postale esistente prima che qualsiasi cambio di e-mail/telefono diventi effettivo; (d) un periodo di attesa di 14 giorni per le modifiche dei metodi di contatto a meno che non siano verificate da un codice spedito per posta; (e) revisione manuale dei passaggi a ProtonMail creato di recente o ad altri domini ad alto rischio; (f) un metodo manuale/alternativo per completare la verifica e presentare i moduli W-9/W-8BEN che non sia condizionato da indicatori del portale, con un SLA di escalation pubblicato (escalation entro 5 giorni lavorativi; risoluzione entro 10 giorni lavorativi); (g) registri di controllo immutabili dei cambi di stato e un intervento di revisione umana; (h) controlli standard del settore per la recapitabilità e l'anti-spoofing (domini dedicati, applicazione di DMARC/SPF/DKIM, disciplina del tracciamento dei link, rimozione di domini simili basati su parole chiave FTX/Kroll/claims); (i) audit annuali indipendenti sulla sicurezza, la recapitabilità e il flusso di lavoro del portale con rapporti disponibili al Tribunale; e (j) monitoraggio finanziato del credito/ID e dei conti di criptovalute e un programma di rimborso delle perdite per phishing per i richiedenti interessati.

92. Il provvedimento richiesto preverrà danni futuri che il solo risarcimento non può rimediare, garantirà un accesso equo alle distribuzioni e allineerà le pratiche di Kroll ai rischi prevedibili unici per i creditori di criptovalute.

93. L'Attore e le Classi non dispongono di un rimedio adeguato in diritto per i danni futuri affrontati dalle ingiunzioni richieste; il risarcimento monetario non può garantire un'amministrazione tempestiva, sicura ed efficace degli obblighi continui dei richiedenti.

94. Il bilanciamento degli interessi e l'interesse pubblico favoriscono il provvedimento ingiuntivo perché protegge i diritti di migliaia di richiedenti di essere ascoltati e di ricevere distribuzioni senza un rischio indebito di frode o espunzione causato da processi difettosi.

95. L'Attore e le Classi chiedono anche il rimborso delle loro ragionevoli spese legali e costi nella misura consentita dalla legge, anche in base alle dottrine del "common fund"/"common benefit" e ai poteri equitativi del Tribunale.

ARBITRATO/RINUNCIA ALL'AZIONE COLLETTIVA

96. Il Portale FTX non è il "Sito" di Kroll come definito nei Termini di Utilizzo di Kroll. L'Attore non ha acconsentito nel Portale FTX ad alcun Termine di Kroll. Il Portale FTX conteneva solo un consenso al trattamento dei dati di FTX; non mostrava alcun Termine di Kroll, nessuna clausola arbitrale e nessuna rinuncia all'azione collettiva. Nella misura in cui Kroll faccia riferimento a un accordo "click-through" separato sul suo EPOC o Sito Kroll, la clausola è limitata ed elettiva, applicandosi solo alle controversie "derivanti da o relative a questi Termini o al nostro Sito", e non vi è alcuna clausola di delega — quindi questo Tribunale decide sull'arbitrabilità. Le pretese dell'Attore derivano dai doveri di amministrazione e sicurezza dei dati di Kroll nominata dal tribunale (violazione di M365; canali di notifica post-violazione; mancanza di un percorso non condizionato per i moduli fiscali), che esistono indipendentemente da qualsiasi uso del sito web e non rientrano in alcuna clausola limitata al sito. In alternativa, imporre l'arbitrato/rinuncia all'azione collettiva come condizione per depositare un Modulo federale 410 è proceduralmente iniquo; e secondo la politica pubblica di New York, la colpa grave non può essere contrattualmente esclusa. Il linguaggio dei Termini su "base individuale" è limitato all'arbitrato; non c'è una rinuncia autonoma all'azione collettiva in tribunale. La clausola di esclusione per l'Incidente di Sicurezza di Kroll nel Piano conferma che si tratta di pretese per illecito di terzi indipendenti contemplate per procedere 'in un altro procedimento', minando qualsiasi teoria basata su soggetti non firmatari.

CONCLUSIONI

PER QUESTI MOTIVI, l'Attore, in proprio e per conto degli altri membri delle Classi proposte nel presente Atto di Citazione, chiede rispettosamente che il Tribunale emetta una sentenza a loro favore e

contro il Convenuto, come segue:

A. Un'Ordinanza che certifichi la presente azione come azione collettiva e nomini l'Attore e i suoi difensori a rappresentare le Classi;

B. Un provvedimento equitativo che richieda la restituzione e la retrocessione dei ricavi illecitamente tratti a causa della condotta illecita del Convenuto;

C. La condanna al risarcimento dei danni effettivi, dei danni emergenti e del lucro cessante, dei danni statuari e delle sanzioni statutarie, in un importo da determinarsi, come consentito dalla legge;

D. La condanna al pagamento di danni punitivi, come consentito dalla legge;

E. Rimedi secondo il DTPA del Texas: danni economici, triplo del danno per violazioni consapevoli/intenzionali, e spese legali ragionevoli e necessarie (DTPA § 17.50(d));

F. GBL di New York §§ 349/350 (in alternativa): danni statuari e spese legali;

G. La condanna al pagamento delle spese legali e dei costi, e altre spese, inclusi gli onorari dei consulenti tecnici;

H. Interessi pre e post-sentenza su qualsiasi importo riconosciuto; e

I. Ogni altro e ulteriore provvedimento che questo tribunale riterrà giusto e opportuno.

Data: 19 agosto 2025

Rispettosamente depositato,

HALL ATTORNEYS, P.C.

A cura di: /s/ Nicholas Andrew Hall

Nicholas Andrew Hall

N. Iscrizione Albo 24069863

nhall@hallattorneys.com

P.O. Box 1370

Edna, Texas 77957

+1 713 428 8967

DIFENSORE DELL'ATTORE E DELLE POTENZIALI CLASSI

