

& IMPORTANT DISCLAIMER

IMPORTANT DISCLAIMER

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

TRANSLATED DOCUMENT

**NO TRIBUNAL DISTRITAL DOS ESTADOS UNIDOS PARA O DISTRITO OESTE DO TEXAS
DIVISÃO DE AUSTIN**

JACOB KEVYN REPKO, individualmente e em nome de todos os outros em situação semelhante,

Autor,

v.

KROLL RESTRUCTURING

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

Ré.

)

) Processo N.º: 1:25-cv-01319

)

)

) PETIÇÃO INICIAL DE AÇÃO COLETIVA

)

)

)

) REQUER JULGAMENTO POR JÚRI

)

)

)

PETIÇÃO INICIAL DE AÇÃO COLETIVA

O Autor Jacob Kevyn Repko ("Autor"), individualmente e em nome de todos os outros em situação semelhante, por meio dos advogados abaixo assinados, alega o seguinte contra a Ré Kroll Restructuring Administration LLC (f/k/a Prime Clerk LLC) ("Kroll" ou "Ré"). Com base em conhecimento pessoal, bem como em informações e crenças, o Autor alega especificamente o seguinte:

NATUREZA DA AÇÃO

1. Esta é uma ação coletiva por violação de dados e administração negligente decorrente do incidente de segurança da Kroll de 19 de agosto de 2023 e de sua subsequente falha em administrar processos e notificações voltados aos credores com o devido cuidado em três grandes falências de criptomoedas — FTX, BlockFi e Genesis.

2. A violação da Kroll expôs (entre outros campos) nomes, endereços, endereços de e-mail, números de telefone, identificadores/valores de créditos e cópias de formulários de prova de crédito — precisamente os metadados que criminosos exploram para visar vítimas de criptomoedas com ataques de phishing e "chave inglesa".

3. Após a violação, a Kroll persistiu em notificações críticas apenas por e-mail (incluindo a 130ª Objeção Omnibus da FTX, verificação de crédito e prazos de formulários fiscais), apesar de (a) imitações de phishing generalizadas que treinaram muitos credores a evitar abrir e-mails da "Kroll" e (b) a capacidade demonstrada da Kroll de enviar cartas via USPS de primeira classe quando optava por fazê-lo — por exemplo, no caso Genesis, onde a Kroll enviou notificações de violação por Correio de Primeira Classe.

4. Os tribunais federais de falência haviam selado as IIP (Informações de Identificação Pessoal) dos credores precisamente para prevenir crimes direcionados a criptomoedas — citando os danos reais vistos na falência da Celsius (ataques de phishing e "chave inglesa"). O processo da Genesis registra essas preocupações em ordens que selam as informações dos clientes.

5. O Autor Jacob Kevyn Repko (Dripping Springs, Texas) apresentou um crédito de cliente da FTX e, em seguida, recebeu a notificação de violação da Kroll em 24 de agosto de 2023. Suas IIP e dados de crédito estavam entre os dados comprometidos.

6. Nos meses que se seguiram, o Portal de Créditos de Clientes da FTX (o "Portal FTX") apresentou mau funcionamento repetidamente: o KYC do Autor mostrava "Verificado", depois voltava para "Em Espera/Não Verificado", impedindo-o de carregar o formulário do IRS (W-9) necessário para receber distribuições, apesar de dezenas de e-mails de suporte.

7. Como o Portal FTX condiciona o carregamento do formulário fiscal à verificação "KYC Verificado", o Autor não pode completar os pré-requisitos finais; sob o plano confirmado e as comunicações do fundo, os créditos podem ser expurgados ou as distribuições perdidas se os formulários fiscais não forem carregados em tempo hábil.

8. O Autor também sofreu perda direta por phishing após a violação: ele transferiu 1.9 ETH de uma conta de exchange para sua carteira quente às 12:43 PM de 3 de julho de 2025 e o valor foi desviado através de um bot de transação automatizado comumente usado para interceptar transferências pendentes para uma carteira não controlada pelo Autor, de acordo com o próprio aviso da Kroll de que os invasores usariam os dados vazados para fazer phishing em contas de criptomoedas.

PARTES

9. O Autor Jacob Repko é uma pessoa física domiciliada no Condado de Hays, Texas. Ele é um cliente-credor da FTX com um crédito listado de \$87.487,93.

10. A Ré Kroll Restructuring Administration LLC é uma LLC de Delaware com operações significativas em todo o país, incluindo escritórios no Texas.

11. Com base em informações e crenças, o Autor também processa os Réus Desconhecidos 1-5, entidades não pertencentes à Kroll atualmente não identificadas que participaram, se for o caso, da verificação voltada aos requerentes ou da recepção de formulários fiscais (incluindo fornecedores terceirizados de KYC). Na medida em que qualquer entidade não pertencente à Kroll controlou os indicadores de status de KYC ou o condicionamento do W-9/W-8 dentro do Portal FTX, o Autor apresenta essas alegações alternativamente e emendará e substituirá os nomes verdadeiros quando identificados. Se a Kroll designar qualquer terceiro responsável, o Autor se juntará oportunamente a tal parte sob as regras de responsabilidade proporcional do Texas.

JURISDIÇÃO E COMPETÊNCIA

12. Este Tribunal tem jurisdição sobre a matéria sob 28 U.S.C. § 1332(d) (CAFA): as classes propostas excedem 100 membros; a controvérsia agregada excede \$5.000.000; existe diversidade mínima (autor do Texas vs. ré de Delaware/Nova York com membros da classe nacionais/internacionais).

13. Este Tribunal tem jurisdição pessoal sobre a Kroll porque a Kroll mantém escritórios em Austin, Dallas e Houston, direciona propositadamente o trabalho de administração/notificação e as comunicações com os requerentes para o Texas, e cometeu atos que causaram danos a um residente do Texas neste Distrito. As reivindicações do Autor surgem de ou se relacionam com essa conduta no foro, e o exercício da jurisdição está de acordo com o devido processo legal.

14. A competência é adequada sob 28 U.S.C. § 1391(b) porque uma parte substancial dos eventos e danos ocorreu neste Distrito: o Autor reside aqui, recebeu as notificações da Kroll aqui, usou o Portal de

Créditos de Clientes da FTX (claims.ftx.com) e depois a Prova de Crédito Eletrônica ("EPOC") da Kroll aqui, e sofreu perda por phishing aqui.

15. Neste momento, o Autor não apresenta reivindicações contra os Devedores, ou qualquer parte liberada pelo plano, e não busca reparação que exija interpretação, modificação ou execução do Plano ou da Ordem de Confirmação. Estas são reivindicações independentes de responsabilidade civil/contrato contra a Kroll, que não é devedora. Esta ação não é um procedimento central; o Autor exige um júri e não consente com a adjudicação em falência.

DEFINIÇÕES

16. "Portal de Créditos de Clientes da FTX" ou "Portal FTX" significa o portal em claims.ftx.com operado para os Devedores/FTX Recovery Trust (com fornecedores) para lidar com KYC/AML e revisão de contas. "Site da Kroll" significa o site da Kroll, incluindo a interface EPOC em restructuring.ra.kroll.com, que recebeu submissões do Formulário 410 de falência e manteve o registro público de créditos. Onde o controle não for claro, o Autor alega alternativamente contra os Réus Desconhecidos a serem substituídos quando identificados.

ALEGAÇÕES DE FATO

A. A Violação da Kroll Abrangeu FTX, Genesis e BlockFi

17. Em ou por volta de 19 de agosto de 2023, um invasor realizou um SIM-swap no telefone de um funcionário da Kroll, acessando os arquivos em nuvem da Kroll com dados de requerentes de cada massa falida. A inteligência de ameaças independente confirma que os campos comprometidos foram posteriormente monetizados e operacionalizados por fraudadores visando requerentes da FTX e transações no mercado secundário.

18. O documento da Kroll no caso Genesis admite que os dados impactados incluíam nomes, números de telefone, endereços, números/valores de créditos, saldos de carteiras/moedas e cópias de provas de crédito.

19. A notificação da BlockFi detalha ainda que data de nascimento, endereço postal e números de carteira de motorista foram envolvidos e relata a identificação tardia pela Kroll de um grande lote de "Arquivos Não Estruturados".

B. Tribunais Selaram as IIP dos Credores Porque Credores de Criptomoedas Enfrentam Vetores de Ataque Únicos

20. No caso Genesis, o tribunal emitiu ordens de selo protegendo os nomes/informações de contato dos credores, referenciando a experiência da Celsius, onde ataques de phishing e "chave inglesa" se seguiram a divulgações públicas.

C. A Kroll Sabia que o E-mail Não Era Seguro, Mas Falhou em Usar o Correio Postal para Notificações Críticas

21. Com base em informações e crenças, a Kroll alertou publicamente os credores da Genesis sobre phishing e enviou notificações de violação por Correio de Primeira Classe para garantir a entrega.

22. No entanto, na FTX, para notificações igualmente (ou mais) consequentes — incluindo os prazos da 130ª Objeção Omnibus (por exemplo, iniciar o KYC até 1º de março de 2025; completar até 1º de junho de 2025) e o prazo do formulário fiscal — a Kroll confiou principalmente no e-mail apenas meses após sua própria violação que desencadeou phishing, sabendo que muitos destinatários não abriam e-mails da "Kroll" por medo de golpes ou os encontrariam em spam/lixo eletrônico. A inteligência de ameaças pública mostra tomadas de conta lideradas por phishing onde os perpetradores alteraram os e-mails dos requerentes para novos endereços do ProtonMail e passaram rapidamente pelos desafios de 2FA — precisamente o ataque que a abordagem apenas por e-mail da Kroll deixou sem mitigação.

23. O Portal FTX condiciona o carregamento do W-9/W-8BEN à verificação KYC. Quando o portal erroneamente reverte um usuário para "Em Espera/Não Verificado", a etapa do formulário fiscal se torna impossível — arriscando o expurgo do crédito ou a perda de distribuições sob os processos do plano comunicados aos credores. Em um ambiente onde os requerentes são treinados para evitar e-mails da "Kroll" devido à imitação ativa, uma etapa de formulário fiscal online e condicionada, sem uma alternativa de Correio de Primeira Classe, não foi razoavelmente calculada para informar ou permitir a conclusão.

24. A ordem de confirmação da FTX prevê expressamente que a Kroll não é liberada ou exculpada por reivindicações de "Incidente de Segurança" e que os danos aos clientes recuperáveis em outro

processo não são limitados pelas distribuições do plano. O Autor solicita respeitosamente que se tome conhecimento judicial desse trecho da ordem de confirmação sob a Fed. R. Evid. 201.

25. Além de ser empregada pelo tribunal de falências sob a notificação do §156(c), a Kroll foi contratada como Consultora Administrativa para realizar serviços de administração de falências sob seus documentos de contratação e a ordem de retenção do Tribunal. Essas funções voltadas aos credores (solicitação/votação/tabulação e tratamento das comunicações dos requerentes) apoiam as obrigações de administração alegadas neste documento.

D. A Experiência do Autor

26. O Autor apresentou seu crédito de cliente usando o Portal FTX e, quando solicitado, registrou o Formulário 410 de falência através do EPOC da Kroll.

27. Ele recebeu a notificação de violação da Kroll confirmando a exposição de seu nome, endereço, e-mail e saldo da conta e alertando sobre phishing direcionado a ativos de criptomoedas.

28. Após lutar com bloqueios e atrasos no portal, o KYC do Autor foi verificado em ou por volta de 3 de novembro de 2023, mas o portal posteriormente reverteu para "Em Espera", bloqueando o carregamento do formulário do IRS; inúmeros e-mails para a Kroll não foram resolvidos.

29. Após a violação, o Autor foi vítima de phishing: 1.9 ETH foram drenados minutos após chegarem à sua carteira quente (chegada às 12:43 PM; saída às 12:49 PM para o endereço do invasor).

30. O Autor detém um crédito listado da FTX de \$87.487,93 e agora enfrenta a perda de parte ou de todo o valor da distribuição porque não pode satisfazer os pré-requisitos do plano devido a falhas no portal e falhas na notificação.

31. O Autor sofreu danos concretos, incluindo: (a) uso indevido real — roubo de 1.9 ETH minutos após a chegada à sua carteira em 3 de julho de 2025; (b) danos de valor-tempo e de distribuição por bloqueio na verificação/submissão de formulário fiscal; (c) custos de mitigação diretos; (d) perda de privacidade/controle de IIP; e (e) risco substancial de uso indevido futuro, dados os padrões de direcionamento a criptomoedas documentados aqui.

E. Uso Indevido Sistemático de Dados Vazados de Requerentes

32. A previsibilidade não é uma abstração: investigadores rastrearam \$5.6 milhões em fraudes explorando dados de créditos da FTX, incluindo vendas na dark web de conjuntos de dados de requerentes e padrões de alteração de e-mail/bypass de 2FA — exatamente os danos que os tribunais buscaram prevenir ao selar as IIP de credores de criptomoedas. A mensagem contrária da Kroll de que nenhuma IIP sensível estava em risco enganou os consumidores sobre a necessidade de tratar cada e-mail da "Kroll" como suspeito e de exigir um backup por correio postal.

33. A inteligência de ameaças independente corrobora que os dados dos requerentes da FTX foram ativamente usados como arma contra credores e contrapartes. De julho a novembro de 2024, investigadores documentaram pelo menos \$5.6 milhões em fraudes ligadas à negociação de créditos da FTX, onde um ator (ou grupo) se passou por detentores de créditos usando selfies alteradas por IA, novas contas do ProtonMail e identificação falsificada.

34. A técnica do ator incluía: (a) endereços do ProtonMail criados recentemente substituindo o e-mail original do requerente; (b) entrada rápida de códigos 2FA, sugerindo tomada de conta; e (c) lavagem através de endereços de depósito da Gate.io, CoinEx e Binance. Esses padrões são consistentes com o comprometimento de credenciais liderado por phishing após o incidente da Kroll.

35. A mesma pesquisa mostra dados de créditos da FTX anunciados em fóruns da dark web, incluindo nomes, telefones, e-mails, detalhes de carteira/transação e outros dados ligados ao crédito — os campos exatos que a Kroll reconheceu terem sido comprometidos (nomes, e-mails, números de telefone, endereços postais, identificadores e saldos de contas e, em alguns casos, datas de nascimento).

36. Os investigadores também observaram alterações de e-mail para contas do ProtonMail pós-fechamento para créditos originalmente abertos com e-mails diferentes, indicando tomada e personificação de contas de requerentes.

37. O relatório documenta caminhos na blockchain de carteiras de personificadores para endereços de depósito da CoinEx e identifica uma carteira intermediária associada à atividade de transação automatizada; ele observa interações com exchanges dos EUA (Coinbase e Kraken) que podem ser intimadas para KYC. Isso evidencia um padrão de fraude coeso e repetível que explora as IIP dos requerentes e as fraquezas do fluxo de trabalho.

38. O relatório observa ainda um erro "Orbeon Forms – Page Not Found" que surgiu durante uma análise de due diligence do Portal FTX — consistente com um fluxo de trabalho de requerente frágil e estados de erro que atores mal-intencionados podem imitar, amplificando a confusão em um ambiente de alto phishing.

F. Declarações Falsas e Omissões Pós-Violação

39. A Kroll, publicamente e em comunicações com os requerentes, minimizou o escopo da violação — afirmando inicialmente que nenhuma IIP sensível havia sido comprometida. Em outras massas falidas que administrou (por exemplo, BlockFi), a Kroll posteriormente divulgou que datas de nascimento estavam contidas em "dados não estruturados", contradizendo suas declarações iniciais. A Kroll também disse aos requerentes da FTX que poderiam continuar interagindo com fluxos de trabalho baseados em e-mail e não alertou que atores mal-intencionados estavam se passando pela Kroll e alterando os endereços de e-mail dos requerentes para contas do ProtonMail recém-criadas para derrotar o 2FA — padrões confirmados por inteligência de ameaças independente. Essas declarações e omissões foram materiais, orientadas ao consumidor e enganosas, e induziram requerentes razoáveis a subestimar o risco, continuar usando canais apenas por e-mail e atrasar uma remediação mais forte, contribuindo para perdas por phishing, danos de valor-tempo e prazos perdidos resultando em créditos expurgados.

ALEGAÇÕES DA CLASSE

40. Classe Global de Credores de Criptomoedas: Todas as pessoas em todo o mundo cujas IIP ou dados de crédito fornecidos à Kroll para os casos de falência da FTX, BlockFi ou Genesis foram acessados, exfiltrados ou razoavelmente em risco no incidente da Kroll de agosto de 2023. A membresia da classe é determinável a partir das listas de notificação da Kroll, registros do EPOC e dos registros de créditos das massas falidas que identificam indivíduos cujos dados a Kroll admite terem sido acessados ou razoavelmente em risco no incidente.

41. Subclasses da Massa Falida: (a) Subclasse FTX; (b) Subclasse BlockFi; e (c) Subclasse Genesis.

O Autor adicionará representantes nomeados para as subclasses BlockFi e Genesis na certificação da classe ou antes dela.

42. Subclasses de Danos (entre as massas falidas): (i) Subclasse de phishing/perda de criptomoedas; (ii) Subclasse de portal/verificação/formulário fiscal (perda por expurgo, perda de valor-tempo e dano administrativo); (iii) Subclasse de dano padrão por violação de dados (invasão de privacidade, custos de mitigação).

43. Numerosidade, comunalidade, tipicidade e adequação estão satisfeitas: questões comuns incluem se a Kroll devia e violou deveres de segurança de dados, adequação da notificação e administração do processo de créditos; se a notificação apenas por e-mail foi razoável pós-violação; e se uma medida cautelar é justificada.

LEI APLICÁVEL

44. Os padrões que regulam a conduta são regidos pela lei de Nova York (a Kroll tem sede e agiu a partir de NY), ou alternativamente pela lei do Texas para residentes e danos no Texas. As reivindicações se baseiam em deveres/atos comuns a todos os membros da classe. Questões de arbitrabilidade são regidas pela FAA; a política pública de Nova York proíbe a exculpação contratual de negligência grave.

FUNDAMENTOS DA AÇÃO

CAUSA DE PEDIR I

Negligência (lei de Nova York; alternativamente, lei do Texas)

45. A Kroll devia ao Autor e às Classes (FTX, BlockFi e Genesis) um dever de exercer cuidado razoável na coleta, armazenamento, transmissão e administração das IIP e dados de crédito dos requerentes; de projetar, operar e apoiar um fluxo de trabalho funcional de verificação/formulário fiscal; e — especialmente após o incidente de 19 de agosto de 2023 — de fornecer notificações razoavelmente calculadas, sob todas as circunstâncias, para informar os requerentes sobre prazos e etapas que afetam direitos e para mitigar riscos previsíveis de phishing e de entrega.

46. Esses deveres surgiram de (a) dos papéis da Kroll como agente de notificação/creditos nomeado pelo tribunal e Consultora Administrativa; (b) ordens judiciais selando as IIP de credores de criptomoedas devido a riscos conhecidos de phishing e segurança física; (c) o próprio conhecimento e alertas da Kroll de que os e-mails expostos dos requerentes seriam alvo de phishing; e (d) o controle da Kroll sobre as

comunicações com os requerentes e a recepção via EPOC; na medida em que uma entidade não pertencente à Kroll controlou os indicadores de status de KYC e o condicionamento do formulário fiscal dentro do Portal FTX, o Autor apresenta essas alegações alternativamente contra os Réus Desconhecidos a serem substituídos quando identificados. Esses deveres são independentes de qualquer contrato e reconhecidos sob a lei de Nova York e do Texas onde a conduta de uma parte cria ou aumenta um risco previsível de roubo de identidade/ativos para uma classe conhecida e finita (requerentes de criptomoedas com IIP seladas), e onde as escolhas de notificação e processo pós-violação são regidas por princípios de devido processo (por exemplo, Mullane; Jones v. Flowers) e pelas ordens de privacidade/notificação do tribunal de falências.

47. A Kroll violou seus deveres, inter alia: (i) permitindo o comprometimento habilitado por SIM-swap de repositórios em nuvem contendo dados de requerentes; (ii) falhando em identificar pronta e completamente todos os armazenamentos de dados impactados; (iii) persistindo — pós-violação — em notificação apenas por e-mail para comunicações que afetam direitos, mesmo que muitos requerentes não pudessem distinguir e-mails legítimos da Kroll de phishing e mesmo que a Kroll tivesse a capacidade e o precedente de enviar Correio de Primeira Classe; (iv) permitindo um fluxo de trabalho de distribuição no qual o carregamento do W-9/W-8BEN era bloqueado a menos que o KYC mostrasse "Verificado" no Portal FTX, enquanto falhava em fornecer um caminho de submissão manual/alternativo via EPOC da Kroll ou por correio/e-mail; (v) falhando em fornecer qualquer caminho de submissão manual/alternativo ou confirmações enviadas por correio para mudanças de status; (vi) fornecendo suporte circular, atrasado ou ineficaz que prolongou e agravou o dano; (vii) falhando, pós-violação, em implementar o endurecimento do controle de alterações (código enviado por correio para o endereço antigo para qualquer alteração de e-mail/telefone; períodos de espera forçados; revisão manual de alterações para contas do ProtonMail criadas após novembro de 2022) apesar da evidência de padrões de tomada de e-mail contra requerentes; e (viii) falhando em implantar monitoramento da dark web e remoções de domínios semelhantes com base em palavras-chave de créditos da FTX/Kroll após ofertas de conjuntos de dados de requerentes serem observadas online.

48. Os riscos que a Kroll criou e falhou em mitigar eram previsíveis: tribunais federais em casos de criptomoedas selaram as IIP de clientes para prevenir ataques de phishing e "chave inglesa"; a aplicação da lei federal e as orientações de segurança alertam os detentores de ativos digitais a manterem as informações de identificação privadas; e a própria Kroll disse aos requerentes que os invasores enviariam e-mails convincentes para tomar o controle de contas e carteiras. Sob essas circunstâncias, o uso exclusivo de e-mail para etapas e prazos críticos de direitos não foi razoável.

49. Os atos e omissões da Kroll foram a causa direta e próxima dos danos do Autor e dos membros da classe. Se não fossem as falhas de segurança da Kroll, a notificação apenas por e-mail, a recusa em enviar correio postal para os prazos da 130ª Objeção Omnibus e o prazo do formulário fiscal, e o portal quebrado e condicionado, o Autor e muitos membros da classe teriam iniciado e completado a verificação e submetido os formulários fiscais em tempo hábil; não teriam seus créditos expurgados ou colocados "em espera", atrasando assim as distribuições do plano; e teriam evitado perdas por phishing e custos de mitigação.

50. O Autor e as Classes sofreram danos incluindo, sem limitação: (a) perdas por phishing/criptomoedas (para o Autor, 1.9 ETH drenados minutos após o recebimento); (b) danos de valor-tempo por atrasos na distribuição causados pela notificação apenas por e-mail e pelos defeitos do portal; (c) expurgo/perda de crédito ligado a prazos de verificação/formulário fiscal perdidos; (d) despesas diretas (monitoramento, endurecimento de dispositivo/carteira, obtenção de documentos) e tempo perdido; e (e) diminuição da privacidade e roubo contínuo de identidade e ativos.

51. O Autor e as Classes buscam indenização por danos compensatórios e consequenciais em um valor a ser provado em julgamento, juntamente com juros pré e pós-julgamento.

CAUSA DE PEDIR II

Lei de Práticas Comerciais Enganosas do Texas—Lei de Proteção ao Consumidor (Tex. Bus. & Com. Code § 17.41 et seq.)

52. O Autor é um consumidor sob o Tex. Bus. & Com. Code §17.45(4) porque buscou e usou serviços — a administração de créditos da Kroll e os serviços voltados aos credores adquiridos para o benefício do Autor pelos Devedores da FTX/FTX Recovery Trust — e esses serviços foram fornecidos ao Autor para permitir que ele reivindicasse e recebesse distribuições sobre seu crédito.

53. A Kroll se envolveu em atos enganosos, incluindo: (1) representar que os serviços tinham características/benefícios que não tinham — a saber, que nenhuma IIP sensível (por exemplo, nome completo, endereço postal, data de nascimento, detalhes de carteira/transação) foi tomada e que os processos por e-mail eram seguros pós-violação; (2) falhar em divulgar informações conhecidas no momento das transações (que IIP sensível estava em "dados não estruturados"; que a personificação/tomada de controle por alteração de e-mail estava ativa) para induzir os requerentes a continuar o fluxo de trabalho apenas por e-mail; e (3) representar direitos/obrigações sob o processo de créditos que eles não tinham — implicando que a notificação apenas por e-mail era razoável e suficiente para prazos críticos de direitos.

54. Na esteira de um incidente de segurança conhecido e de uma campanha de phishing ativa, persistir com a notificação apenas por e-mail para prazos críticos de direitos e omitir um suporte postal e um canal de submissão manual de formulário fiscal foi um curso de ação inescrupuloso que se aproveitou grosseiramente da falta de conhecimento e da incapacidade dos requerentes de se protegerem.

55. As violações da DTPA pela Kroll foram a causa produtora dos danos do Autor, incluindo (i) o roubo de 1.9 ETH após phishing, (ii) danos de valor-tempo/distribuição por bloqueio na verificação e submissão de formulário fiscal, e (iii) custos de mitigação e perda de privacidade/controlado de IIP.

56. A Kroll agiu com conhecimento e, em alguns aspectos, intencionalmente: ela sabia, por suas próprias investigações em outras massas falidas (por exemplo, BlockFi), que IIP sensível existia em "dados não estruturados", mas disse aos requerentes o contrário e falhou em ajustar a notificação e os fluxos de trabalho de acordo.

57. O Autor busca danos econômicos, honorários advocatícios, custos e danos triplos por violações conscientes/intencionais sob a DTPA do Texas.

58. O Autor enviou ou está enviando contemporaneamente a notificação pré-processual. Na medida em que a notificação não foi viável devido a limitações iminentes e à necessidade de medida cautelar, o Autor solicita que o Tribunal suspenda a reivindicação da DTPA por 60 dias a partir da citação para permitir discussões de cura, conforme previsto em lei.

CAUSA DE PEDIR III

Atos Enganosos e Desleais de Nova York (alternativamente)

59. A Kroll se envolveu em atos e práticas enganosas orientadas ao consumidor, incluindo o envio de notificações de caso e comunicações com requerentes enganosas e voltadas ao público, minimizando a violação (afirmando que não havia IIP sensível), falhando em divulgar fatos materiais (IIP presente em arquivos e em "dados não estruturados"; personificação ativa) e incentivando a continuação de comunicações apenas por e-mail em um ambiente de phishing ativo. Esses atos foram enganosos de maneira material e prejudicaram o Autor. O Autor busca danos reais, danos estatutários, honorários advocatícios razoáveis e medida cautelar sob a Lei Geral de Negócios de Nova York §§ 349(h) e 350-e.

CAUSA DE PEDIR IV

Negligência Grave

60. A conduta da Kroll foi mais do que negligência comum. Sabendo que as IIP dos requerentes haviam sido expostas, e sabendo que os requerentes estavam sendo ativamente alvo de phishing, a Kroll persistiu conscientemente em mensagens apenas por e-mail, com muitos links e propensas a imitações para prazos que afetam direitos; recusou-se a mudar para o correio postal em escala, mesmo tendo a capacidade e tendo usado o correio para outras comunicações críticas; e continuou a condicionar a submissão de formulários fiscais a um portal de créditos não confiável que repetidamente alternava os usuários entre "Verificado" e "Em Espera" sem explicação — mesmo após a inteligência de terceiros documentar a personificação contínua, tomadas de controle por alteração de e-mail e rotas de lavagem usando dados de requerentes.

61. A falha da Kroll em implantar salvaguardas óbvias — Correio de Primeira Classe para notificações críticas de direitos, confirmações enviadas por correio de mudanças de status, um caminho manual não condicionado para formulários fiscais, endurecimento do controle de alterações (códigos enviados por correio para o endereço existente; períodos de espera; revisão manual de mudanças para contas do ProtonMail criadas recentemente) e monitoramento da dark web — foi um desvio extremo do cuidado comum diante de uma alta probabilidade de dano grave a uma população cujas IIP foram seladas precisamente para evitar phishing e direcionamento físico.

62. A conduta grosseiramente negligente da Kroll foi um fator substancial na causa dos danos do

Autor e das Classes e apoia a concessão de danos punitivos para punir e dissuadir condutas semelhantes.

63. O Autor e as Classes buscam danos punitivos em um valor suficiente para refletir a repreensibilidade da conduta da Kroll e para dissuadir futuras violações.

CAUSA DE PEDIR V

Quebra de Contrato Implícito (Privacidade e Administração de Créditos)

64. Ao solicitar e aceitar as IIP e as submissões de crédito do Autor e dos membros da classe e ao exigir que eles usassem o Portal FTX (KYC/revisão) e o EPOC da Kroll (apresentação de crédito) para participar do processo de créditos da falência, a Kroll celebrou contratos implícitos para (a) salvaguardar essas informações com segurança razoável, (b) administrar as etapas de verificação e formulário fiscal com cuidado razoável, e (c) fornecer canais razoavelmente projetados para garantir que os requerentes pudessem completar as etapas que afetam direitos.

65. O Autor e os membros da classe cumpriram sua parte ao fornecer informações precisas e seguir as instruções da Kroll. Eles esperavam razoavelmente que a Kroll protegeria seus dados e forneceria um processo funcional e seguro para completar a verificação e carregar os formulários fiscais.

66. A Kroll violou essas promessas implícitas ao permitir o acesso não autorizado aos dados dos requerentes; ao continuar a usar notificações apenas por e-mail em um ambiente de phishing conhecido; ao persistir em um fluxo de trabalho defeituoso e condicionado sem um caminho alternativo; e ao falhar em fornecer uma opção de submissão manual, não condicionada ou confirmações enviadas por correio para mudanças de status que afetam direitos.

67. Como resultado direto e próximo, o Autor e os membros da classe sofreram os danos descritos acima, incluindo perda por phishing, danos de valor-tempo e de distribuição, e custos diretos.

68. O Autor e as Classes buscam indenização, restituição e toda outra reparação apropriada pela quebra de contrato implícito da Kroll.

CAUSA DE PEDIR VI

Empreendimento Negligente (Restatement (Second) of Torts § 324A)

69. A Kroll se comprometeu a prestar serviços que sabia serem necessários para a proteção do Autor e das Classes — a saber, salvaguardar as IIP dos requerentes e administrar o fluxo de trabalho de verificação/formulário fiscal e as notificações que afetam direitos.

70. A Kroll realizou esse empreendimento negligentemente ao usar notificação apenas por e-mail pós-violação; recusando-se a enviar correio postal para os prazos da 130ª Objeção Omnibus e o prazo do formulário fiscal; condicionando a submissão de formulários fiscais a um fluxo de trabalho não confiável e condicionado por status; e falhando em fornecer um caminho alternativo ou confirmações enviadas por correio.

71. O desempenho negligente da Kroll aumentou o risco de dano ao Autor e aos membros da classe (notificações perdidas ou ignoradas, bloqueios por mudança de status, phishing) e foi um fator substancial nas perdas resultantes.

72. O Autor e muitos membros da classe confiaram no empreendimento da Kroll — usando o Portal FTX e as comunicações/EPOC da Kroll para requerentes conforme instruído e renunciando a outras etapas porque a Kroll era o canal exclusivo para verificação e administração de créditos.

73. O Autor e as Classes têm direito a indenização por danos proximamente causados pelo empreendimento negligente da Kroll.

CAUSA DE PEDIR VII

Notificação e Processamento de Créditos Negligentes Pós-Violação

74. Após o incidente de 19 de agosto de 2023, a Kroll tinha um dever aumentado de mitigar danos previsíveis e de fornecer notificação e acomodações de processo razoavelmente calculadas para alcançar os requerentes e permitir o cumprimento oportuno de etapas que afetam direitos.

75. A Kroll violou esse dever ao continuar a confiar na notificação apenas por e-mail — apesar do phishing generalizado e da filtragem de spam direcionada a e-mails semelhantes aos da Kroll — e ao falhar em mudar para o correio postal para as comunicações mais consequentes, incluindo os prazos da 130ª Objeção Omnibus da FTX (para começar até 1º de março de 2025 e completar até 1º de junho de 2025) e o prazo do formulário fiscal. O plano confirmado não continha datas fixas no texto do plano; portanto, a escolha do canal da Kroll tornou essas notificações determinantes para o resultado. Muitos requerentes razoáveis não abriram e-mails da Kroll porque fazê-lo parecia "roleta russa" durante

campanhas de phishing ativas; muitas notificações foram para pastas de lixo/spam e não foram vistas.

76. Independentemente, a FTX operou um portal que bloqueava a submissão do W-9/W-8BEN a menos que "KYC Verificado", mas o sistema erroneamente revertia usuários verificados para "Em Espera/Não Verificado", sem substituição manual, sem confirmação enviada por correio de mudanças de status e sem caminho de submissão alternativo — garantindo o não cumprimento evitável.

77. As comunicações de suporte da Kroll agravaram essas falhas — emitindo mensagens padronizadas de "tente novamente" e "corrigido", redirecionando os requerentes para outras caixas de entrada e não fornecendo uma solução duradoura — enquanto os prazos de expurgo e de formulário fiscal se aproximavam.

78. A Kroll declarou falsamente que IIP sensível não estava implicada e mais tarde reconheceu datas de nascimento em "dados não estruturados" em outra massa falida de criptomoedas (BlockFi), reduzindo assim a vigilância e aumentando o sucesso do phishing.

79. Como resultado direto e próximo da notificação e processamento de créditos negligentes da Kroll, o Autor e os membros da classe perderam ou não conseguiram completar os requisitos de verificação e formulário fiscal que de outra forma teriam satisfeito, sofreram perdas por phishing e incorreram em danos de valor-tempo e administrativos.

80. O Autor e as Classes buscam indenização por esses danos e uma declaração de que as práticas de notificação/processamento pós-violação da Kroll foram irrazoáveis e ilegais sob as circunstâncias.

81. O Autor e as Classes buscam ainda medida cautelar exigindo notificação multicanal (e-mail e correio de primeira classe com URLs digitadas/códigos únicos), confirmações enviadas por correio para qualquer mudança de status que afete direitos, janelas de cura definidas antes do expurgo e um canal manual/alternativo para verificação e submissão de formulário fiscal. A Kroll continua a administrar as comunicações e registros voltados aos credores relacionados a essas massas falidas, então o risco de dano futuro é contínuo na ausência de salvaguardas ordenadas pelo tribunal.

CAUSA DE PEDIR VIII

Declaração Falsa Negligente (declarações de processo pós-violação)

82. A Kroll, em comunicações pós-violação, representou que os erros de verificação foram "corrigidos", que os requerentes deveriam "tentar novamente", ou que o status era "Verificado", quando o sistema continuava a reverter para Em Espera/Não Verificado e a bloquear a submissão de formulários fiscais. O papel da Kroll como agente de créditos/notificação nomeado pelo tribunal e Consultora Administrativa a colocou em uma posição de acesso único e confiável às informações dos credores e ao controle do processo, criando uma relação especial suficiente para suportar a responsabilidade por declaração falsa negligente.

83. A Kroll forneceu essas informações no curso de seus deveres de administração profissional e falhou em exercer cuidado razoável. O Autor e os membros da classe confiaram justificadamente ao continuar com o mesmo fluxo de trabalho quebrado e renunciando a alternativas de escalonamento, causando prazos perdidos, perdas de valor-tempo e expurgo.

84. O Autor busca indenização por danos proxivamente causados por essa confiança.

CAUSA DE PEDIR IX

Enriquecimento Ilícito (alternativamente)

85. A Kroll recebeu compensação substancial por servir como agente de notificação/créditos e Consultora Administrativa em todas as massas falidas de criptomoedas, enquanto externalizava os custos e riscos de sua segurança deficiente e administração pós-violação para os requerentes.

86. Seria iníquo para a Kroll reter esses benefícios sem reembolsar as perdas que causou e sem financiar medidas corretivas (incluindo monitoramento, melhorias de segurança, re-notificação e reabertura de janelas de submissão).

87. O Autor alega enriquecimento ilícito alternativamente às suas reivindicações contratuais e de responsabilidade civil, na medida em que o Tribunal considere que nenhum contrato executável rege os deveres da Kroll para com os requerentes.

88. O Autor e as Classes buscam restituição e devolução de benefícios ilícitos e compensações de taxas proporcionais aos danos causados.

CAUSA DE PEDIR X

Medida Declaratória e Cautelar (28 U.S.C. §§ 2201-02)

89. Existe uma controvérsia real e justificável sobre as obrigações contínuas da Kroll de proteger os dados dos requerentes, de dar notificação adequada de etapas que afetam direitos e de operar um processo funcional de verificação/formulário fiscal que não bloqueie arbitrariamente requerentes cumpridores.

90. O Autor busca uma declaração de que a notificação apenas por e-mail e o portal condicionado pós-violação da Kroll foram irrazoáveis sob as circunstâncias e que a Kroll deve empregar processos razoavelmente calculados para alcançar e proteger os requerentes no futuro.

91. O Autor também busca uma liminar permanente exigindo que a Kroll, por não menos de três (3) anos, implemente: (a) notificação multicanal (e-mail e Correio de Primeira Classe) para qualquer prazo que afete direitos, com URLs digitadas/códigos de acesso únicos e sem links clicáveis; (b) confirmações enviadas por correio de qualquer mudança de status de verificação e uma janela de cura mínima de 30 dias antes do expurgo ou perda; (c) endurecimento do controle de alterações: códigos de uso único enviados por correio para o endereço postal existente antes que qualquer alteração de e-mail/telefone entre em vigor; (d) um período de espera de 14 dias para alterações de método de contato, a menos que verificado por um código enviado por correio; (e) revisão manual de mudanças para contas do ProtonMail ou outros domínios de alto risco criados recentemente; (f) um método manual/alternativo para completar a verificação e submeter o W-9/W-8BEN que não seja condicionado por indicadores do portal, com um SLA de escalonamento publicado (escalonamento em 5 dias úteis; resolução em 10 dias úteis); (g) registros de auditoria imutáveis de mudanças de status e uma substituição por revisão humana; (h) controles de entrega e anti-spoofing padrão da indústria (domínios dedicados, aplicação de DMARC/SPF/DKIM, disciplina de rastreamento de links, remoções de domínios semelhantes com base em palavras-chave da FTX/Kroll/créditos); (i) auditorias anuais independentes de segurança, entrega e fluxo de trabalho do portal com relatórios disponíveis para o Tribunal; e (j) monitoramento financiado de crédito/ID e contas de criptomoedas e um programa de reembolso de perdas por phishing para os requerentes afetados.

92. A reparação solicitada prevenirá danos futuros que apenas a indenização não pode remediar, garantirá o acesso justo às distribuições e alinhará as práticas da Kroll com os riscos previsíveis únicos dos credores de criptomoedas.

93. O Autor e as Classes não têm um remédio adequado na lei para os danos prospectivos abordados pelas liminares solicitadas; a reparação monetária não pode garantir a administração oportuna, segura e eficaz das obrigações contínuas dos requerentes.

94. O equilíbrio das equidades e o interesse público favorecem a medida cautelar porque protege os direitos de milhares de requerentes de serem ouvidos e de receberem distribuições sem risco indevido de fraude ou expurgo causado por processos defeituosos.

95. O Autor e as Classes também buscam seus honorários advocatícios e custos razoáveis na medida permitida por lei, incluindo sob as doutrinas de fundo comum/benefício comum e os poderes equitativos do Tribunal.

ARBITRAGEM/RENÚNCIA A AÇÃO COLETIVA

96. O Portal FTX não é o "Site" da Kroll conforme definido nos Termos de Uso da Kroll. O Autor não consentiu no Portal FTX com quaisquer Termos da Kroll. O Portal FTX continha apenas um consentimento de processamento de dados da FTX; não exibia Termos da Kroll, nenhuma cláusula de arbitragem e nenhuma renúncia a ação coletiva. Na medida em que a Kroll aponta para um clique separado em seu EPOC ou Site da Kroll, a cláusula é restrita e eletiva, aplicando-se apenas a disputas "decorrentes de ou relacionadas a estes Termos ou ao nosso Site", e não há cláusula de delegação — portanto, este Tribunal decide a arbitrabilidade. As reivindicações do Autor decorrem dos deveres de administração e segurança de dados nomeados pelo tribunal da Kroll (violação do M365; canais de notificação pós-violação; falta de um caminho não condicionado para formulários fiscais), que existem independentemente de qualquer uso de site e estão fora de qualquer cláusula limitada ao site. Alternativamente, extrair a arbitragem/renúncia a ação coletiva como condição para apresentar um Formulário federal 410 é processualmente inescrupuloso; e sob a política pública de Nova York, a negligência grave não pode ser contratualmente desculpada. A linguagem dos Termos sobre "base individual" está confinada à arbitragem; não há renúncia autônoma a ação coletiva em tribunal. A exceção do Plano para Incidentes de Segurança da Kroll confirma que estas são reivindicações de responsabilidade civil de terceiros independentes contempladas para prosseguir 'em outro processo', minando qualquer teoria de não signatário.

PEDIDOS

PELO EXPOSTO, o Autor, individualmente e em nome dos outros membros das Classes propostas nesta Petição Inicial, solicita respeitosamente que o Tribunal profira sentença em seu favor e contra a Ré, da seguinte forma:

A. Por uma Ordem certificando esta ação como uma ação coletiva e nomeando o Autor e seu advogado para representar as Classes;

B. Por reparação equitativa exigindo restituição e devolução das receitas indevidamente retidas devido à conduta ilícita da Ré;

C. Pela concessão de danos reais, danos compensatórios, danos estatutários e penalidades estatutárias, em um valor a ser determinado, conforme permitido por lei;

D. Pela concessão de danos punitivos, conforme permitido por lei;

E. Remédios da DTPA do Texas: danos econômicos, danos triplos por violações conscientes/intencionais e honorários advocatícios razoáveis e necessários (DTPA § 17.50(d));

F. GBL de Nova York §§ 349/350 (alternativa): danos estatutários e honorários advocatícios;

G. Pela concessão de honorários advocatícios e custos, e outras despesas, incluindo honorários de peritos;

H. Juros pré e pós-julgamento sobre quaisquer valores concedidos; e

I. Qualquer outra reparação que este tribunal considere justa e adequada.

Data: 19 de agosto de 2025

Respeitosamente submetido,

HALL ATTORNEYS, P.C.

Por: /s/ Nicholas Andrew Hall

Nicholas Andrew Hall

Nº de Inscrição na Ordem: 24069863

nhall@hallattorneys.com

P.O. Box 1370

Edna, Texas 77957

+1 713 428 8967

ADVOGADO DO AUTOR E DAS CLASSES PROPOSTAS

