KRONENBERGER ROSENFELD, LLP
Karl S. Kronenberger (Bar No. 226112)
Galen K. Cheney (*pro hac vice* forthcoming)
Leah Rosa Vulić (Bar No. 343520)
548 Market St., #85399
San Francisco, CA 94104
Telephone: (415) 955-1155
Facsimile: (415) 955-1158
karl@kr.law
galen@kr.law
leah@kr.law

Attorneys for Plaintiff John Doe

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN FRANCISCO
UNLIMITED CIVIL

JOHN DOE, an individual,

Plaintiff,

v.

PAYWARD VENTURES, INC., a Delaware corporation, **d/b/a KRAKEN**; **PAYWARD, INC.**, a Delaware corporation; **PAYWARD EUROPE SOLUTIONS LTD.**, a Irish private limited company, **d/b/a KRAKEN**; and **JOHN ROES 1-100**, inclusive,

Defendants.

Case No.

CGC-26-634771

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

DEMAND FOR JURY TRIAL

EXCEEDS $35,000

ACTION BASED ON CIVIL CODE SECTION 1708.89

Plaintiff John Doe ("Plaintiff" or "Doe"), who proceeds in this action pseudonymously pursuant to Cal. Civ. Code §1708.89(e)(1), by and through his undersigned counsel, states and alleges as follows:

INTRODUCTION

1. This is an action arising from a catastrophic data breach in which Defendants PAYWARD VENTURES, INC., PAYWARD, INC., and PAYWARD EUROPE SOLUTIONS LTD. (collectively "Kraken" or the "Kraken Defendants") negligently, recklessly, and in breach of their fiduciary duties, disclosed Plaintiff JOHN DOE's complete personal identifying information and account details to international organized criminals; responded to an unsophisticated spoofed email purportedly sent from an Italian law enforcement agency; and released Plaintiff's data without taking even basic steps to verify the request's authenticity.

2. Kraken released this sensitive personal information even though it knew Plaintiff was a high-value cryptocurrency account holder whose holdings made him a prime target for criminal activity, including the well-known threat of so-called "$5 wrench attacks" (physical violence to extract cryptocurrency credentials).

3. The Roe Defendants thereafter used Kraken's unlawfully disclosed data to perpetrate a sophisticated reconnaissance operation designed to gather intelligence for kidnapping and cryptocurrency extortion. This criminal operation included:

a. A 30-minute phone call on July 19, 2025, during which the criminals impersonated Kraken and demonstrated complete knowledge of Plaintiff's personal information obtained from Kraken;

b. Explicit threats of physical violence ("we don't want you getting whacked over the head with a 5 dollar wrench" and threats that the criminals "could beat the seed phrase out of [Plaintiff]");

c. Coordinated physical surveillance and attempted forced entry at Plaintiff's apartment;

d. Ongoing targeting that has forced Plaintiff to separate from his family,

including from his wife and children, and move and relocate several times to different countries, due to the ongoing security threat.

4. Kraken failed to notify Plaintiff of the breach for 39 days after criminals had already used the data against him—a delay that violated state and federal data breach notification requirements and allowed the criminal operation to progress unimpeded.

5. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff and his family have suffered significant harm including: disruption of family life; harm to Plaintiff's business ventures; severe psychological trauma; and ongoing security threats requiring ongoing protective measures.

6. On or around January 7, 2026, while this matter was pending, Nick Percoco, Chief Security Officer of Kraken, appeared in a documentary interview in which he made admissions demonstrating Kraken's sophisticated understanding of how breached customer data gets weaponized by criminals—the exact scenario underlying this Complaint. Despite this knowledge, Kraken failed to implement adequate safeguards to protect customers like Plaintiff.

7. Plaintiff brings this action to regain control of his life, which has been shattered by Kraken's misconduct. Plaintiff seeks to recover damages for the devastating harm he and his family have suffered, to obtain equitable relief to prevent further dissemination of his personal information, to obtain equitable relief requiring Defendant Kraken to implement adequate security measures to prevent future breaches and protect its customers at large, and to hold Defendants accountable for their unlawful conduct.

PARTIES

8. Plaintiff JOHN DOE is proceeding pseudonymously pursuant to California Civil Code section 1708.89(e)(1), which authorizes a plaintiff in a civil proceeding for doxing to proceed using a pseudonym and to exclude or redact identifying characteristics from pleadings and documents. Plaintiff is filing contemporaneously with this Complaint a confidential information form containing his true name and identifying characteristics, which the Court shall keep confidential pursuant to Civil Code section 1708.89(e)(1).

9. Plaintiff is an individual who, at all times relevant to the underlying events, maintained a cryptocurrency account with Defendant Kraken and was a resident of Singapore.

10. Defendant PAYWARD VENTURES, INC. is a Delaware corporation with its principal place of business in San Francisco, California during most if not all of the applicable time period. Payward Ventures, Inc. does business as "Kraken" and operates a digital asset exchange platform. Payward Ventures, Inc. is registered to do business in California.

11. Defendant PAYWARD, INC. is a Delaware corporation with its principal place of business in San Francisco, California. Payward, Inc. is affiliated with Payward Ventures, Inc. and is involved in the operation of the Kraken digital asset exchange. Payward, Inc. is registered to do business in California.

12. Defendant PAYWARD EUROPE SOLUTIONS LTD. ("PESL") is a private limited company incorporated in Ireland, and a wholly-owned subsidiary of Payward Europe Limited with its principal place of business in Ireland, which in turn is whole-owned by PAYWARD, INC.

13. Payward, Inc., a Delaware, USA corporation, is also the parent company of a worldwide group of subsidiaries (the "Payward Group'', the "Kraken Group" or the "Group" collectively doing business as "Kraken").

14. Defendants PAYWARD VENTURES, INC, PAYWARD, INC., and PAYWARD EUROPE SOLUTIONS LTD. are collectively referred to herein as "Kraken" or "Kraken Defendants."

15. Defendants ROES 1 through 100, inclusive (the "Roe Defendants" or "Roes"), are individuals or entities whose true names and capacities are presently unknown to Plaintiff. Plaintiff is informed and believes, and on that basis alleges, that the Roe Defendants include the individuals and entities who:

a. Sent a spoofed email, purportedly from an Italian law enforcement agency to Kraken, using the trademark and logo of an Italian law enforcement agency;

b. Impersonated Italian law enforcement officials in email to Kraken, and impersonated Kraken employees over the phone to Plaintiff;

c. Used Plaintiff's personal information obtained through the spoofed email to contact Plaintiff on July 19, 2025;

d. Conducted physical surveillance of Plaintiff's apartment;

e. Attempted unauthorized entry to Plaintiff's apartment;

f. Engaged in ongoing targeting and harassment of Plaintiff and his family;

g. Otherwise participated in or aided and abetted the criminal conspiracy to obtain Plaintiff's information and use it for purposes of harassment, intimidation, extortion, and kidnapping.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to California Constitution, Article VI, Section 10, as this is a civil action in which the matter in controversy exceeds the jurisdictional minimum. To wit, Plaintiff seeks monetary damages in excess of $35,000, non-monetary relief, injunctive relief, attorney's and punitive damages.

18. This Court has personal jurisdiction over Defendants Payward Ventures, Inc. and Payward, Inc. because they are Delaware corporations that at relevant times were registered to do business in California with their principal places of business in San Francisco, California, and because they engaged in substantial business activities in California that give rise to this action.

19. This Court has personal jurisdiction over Defendant PESL because it engaged in substantial activities in California that give rise to this action. To wit, Plaintiff's data and personal identifying information was held and maintained by Payward Ventures, Inc. and Payward, Inc. in California. Further, the Kraken Defendants', including PESL's, unlawful release of Plaintiff's data and personal identifying information to the Roe Defendants, allowed the Roe Defendants to engage in their unlawful doxing activities as described herein in violation of Cal. Civ. Code §1708.89.

20. This Court has personal jurisdiction over the Roe Defendants because they

engaged in substantial activities in California that give rise to this action.

21. Venue is proper in San Francisco County pursuant to California Code of Civil Procedure sections 395 and 395.5 because:

a. At relevant times Defendants Payward, Inc. and Payward Ventures, Inc., who held and maintained Plaintiff's data and personal identifying information in connection with Plaintiff's Kraken account, maintained their principal places of business in San Francisco County;

b. A substantial portion of the acts and omissions giving rise to this action occurred in San Francisco County;

c. The Terms of Service governing the relationship between Plaintiff and Kraken, which Plaintiff entered into in October 2019 and which were in effect at all relevant times, provide that "the state or federal courts in San Francisco, California have exclusive jurisdiction over any appeals of an arbitration award and over any suit between the parties not subject to arbitration";

d. This action seeks equitable relief for unlawful disclosure of personal identifying information in response to a spoofed email purportedly from an Italian law enforcement agency containing the logo and trademark of the law enforcement agency. Such claims are exempt from the arbitration provision in Kraken's Terms of Service as detailed in paragraph 23 of the terms. A true and correct copy of the October 2019 Terms of Service are attached hereto as **Exhibit A**.

FACTUAL ALLEGATIONS

Background on Cryptocurrency and $5 Wrench Attacks

22. Cryptocurrency is a form of digital or virtual currency that uses cryptography for security and operates using decentralized blockchain technology.

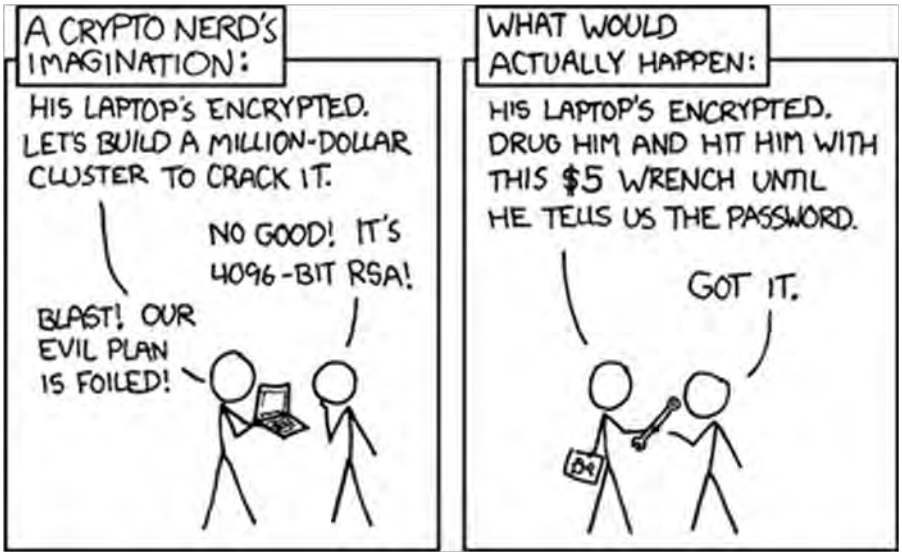
23. Unlike traditional financial assets held by banks or brokers, cryptocurrency is often held with "self-custody" methods by individual owners using private cryptographic keys (called "private keys" or "seed phrases") that provide exclusive access to the digital

assets.

24. Cryptocurrency private keys or seed phrases are analogous to bearer bonds, in that whoever is in possession of them can unilaterally exercise full control over the underlying asset, with no further proof of identity or ownership required.

25. Because cryptocurrency transactions are irreversible and often anonymous, cryptocurrency holders are prime targets for criminals seeking to steal digital assets.

26. A well-known threat in the cryptocurrency community is the "wrench attack" or "$5 wrench attack," which is a term originating from a 2014 XKCD webcomic depicting how physical coercion with a simple tool (a "$5 wrench") can bypass even the most sophisticated encryption by targeting the person who holds the password or private key.



27. Rather than attempting to hack digital security systems, criminals use violence or threats of violence to force cryptocurrency holders to transfer their digital assets, reveal their private keys, or surrender seed phrases that provide the attackers with complete control over their wallets. These attacks have increased dramatically alongside rising cryptocurrency valuations, with violent incidents correlating closely with total crypto market capitalization.

28. In the United States, multiple high-profile cases have demonstrated the severity of this threat:

- In May 2025, two men were charged with kidnapping and torturing an Italian

businessman for approximately 17 days in a Manhattan townhouse, subjecting him to electric shocks, threatening to throw him over a ledge, and ultimately forcing him to provide access to his Bitcoin wallet.

- In 2024, the Department of Justice charged 12 individuals in a racketeering conspiracy involving over $263 million in stolen cryptocurrency, including a coordinated home invasion in New Mexico where an assailant broke into a victim's residence to steal a hardware wallet while an accomplice remotely monitored the victim's location through their iCloud account.
- In November 2025, an assailant invaded a San Francisco residence, tied up the victim, and stole approximately $11 million worth of cryptocurrency using digital keys stored on the property.

29. Europe has also seen a sharp rise in wrench attacks, led by France, which recently recorded 11 such incidents—the highest of any country—and suffered four attempted kidnappings within just four days in early January 2026. Notable European incidents include:

- In January 2025, Ledger co-founder David Balland and his wife were kidnapped in Vierzon, France, during which the suspects severed Balland's finger while making ransom demands.
- Attackers assaulted a victim at the Peninsula Hotel in Paris and stole a hard drive containing €2 million worth of Bitcoin.
- In January 2026, a crypto investment executive and his family were beaten and bound with cable ties by three armed intruders in Verneuil-sur-Seine.
- Also in January 2026, a 43-year-old man was kidnapped from his home in Saint-Léger-sur-Cholet, tied up, assaulted, and abandoned 50 kilometers away.

30. As the European privacy face of Kraken, and recipient of both legitimate and illegitimate requests for consumer information, PESL: a) knows the risks of $5 wrench attacks; b) knows the risks of illegitimate requests for private consumer information; and c) is the sole gate-keeper preventing private consumer information from being made public.

31. Cryptocurrency exchanges like Kraken are well aware of the threat of personal violence. Indeed, on or around January 7, 2026, Nick Percoco, Chief Security Officer of Kraken, appeared in a documentary[1] in which he discussed how criminals use leaked exchange data to contact victims urgently, create fear about compromised accounts, and steal assets.

32. Percoco explained that he and Kraken were aware that organized crime groups and the targeting physically their customers and employees of Kraken, including himself: "there are a lot of people trying to get me [physically]."[2]

33. In the documentary, Percoco positioned Kraken as having a security culture "far higher" than competitors and claimed that employees from other exchanges have provided feedback about Kraken's "superior practices." (*Id*.)

34. Percoco's statements demonstrate that Kraken had sophisticated understanding of the threat model, describing how breached customer data is weaponized by criminals to target victims. This advanced knowledge of the criminal modus operandi makes Kraken's failures in this case all the more egregious.

35. High value cryptocurrency holders like Plaintiff face particular risk of kidnapping, extortion, and violence, as criminals know that cryptocurrency transfers are immediate and irreversible, providing a window of 6-24 hours before law enforcement can effectively respond.

36. This threat is not theoretical. In recent years, there have been numerous documented cases of cryptocurrency holders being kidnapped, tortured, and in some cases killed, including the case of the CEO of Ledger (an industry-leading cryptocurrency hardware wallet company) who was kidnapped in France and had his finger severed.

//

//

[1] Nick Percoco & Kitboga, The Anatomy of a Crypto Scam, YouTube (Oct. 10, 2025), https://youtu.be/uLpCI6CV3Uw

[2] *Id*.

Kraken: A "Security Company" Where No One Is Safe

A. Kraken falsely portrays itself as an industry leader while not following basic privacy and security standards.

37. Kraken is a cryptocurrency exchange. It advertises itself to consumers (its customers and potential customers) as a bedrock of security of both digital assets and customer information, stating: "Security is embedded in every company decision, and protecting client funds and personal information is central to Kraken's operations."[3]

38. Kraken even boldly states: "In many respects, Kraken is a security company that operates a crypto exchange. Kraken's absolute focus on security above everything has helped to keep clients' funds safe and the platform secure despite being under constant attack."[4]

39. Kraken also states: "Security is not just about keeping the crypto we hold safe. The personal identifying information we maintain is just as valuable. Attackers are just as eager to have your personal data as they are your private keys."[5]

40. Kraken's Chief Security Officer represented: "Kraken is world-renowned for our commitment to security. I look forward to leading the industry in security and working to improve the entire ecosystem at the same time!" and "My vision for Kraken is to expand upon the strong, industry leading security foundation we already have in place."[6]

41. Kraken further represents that, "For more than a decade, we've been building an industry leading security practice led by some of the top security experts in the world" with "Industry-leading data security practices."[7]

---

[3] Kraken Learn Team, *Kraken vs Coinbase: How These Crypto Exchanges Compare*, Kraken (Sept. 4, 2025), https://www.kraken.com/learn/kraken-vs-coinbase

[4] *Id.*

[5] Kraken Blog, *How Kraken Manages Client Security*, Kraken Blog (Apr. 5, 2023), https://blog.kraken.com/crypto-education/security-at-kraken

[6] Nick Percoco, *A Letter from Kraken's Chief Security Officer – Nick Percoco*, KRAKEN BLOG (May 4, 2023), https://blog.kraken.com/product/security/a-letter-from-krakens-chief-security-officer-nick-percoco

[7] *Announcing the 2024 Kraken Transparency Report*, KRAKEN BLOG (Feb. 18, 2025), https://blog.kraken.com/news/2024-kraken-transparency-report.

42. Kraken's representations about being an industry leader of security practices are materially false. As described *infra*, Kraken failed to follow basic industry standards, let alone set or lead those standards. For example, Kraken disclosed Plaintiff's data through a facially defective and bogus email request as described, despite where, seven months prior, the FBI warned that criminals were "gaining access to compromised US and foreign government email addresses and using them to conduct fraudulent emergency data requests" and specifically recommended "contacting the sender and originating authority" for verification.[8] Industry-standard authentication platforms report that approximately 30% of seemingly legitimate law enforcement requests fail second-level verification.[9] Kraken's practice described *infra* of accepting email domain appearance without verification falls below minimum industry standards, not "industry-leading" practice.

B. Kraken falsely claims to adhere to information security standards set out in professional certifications.

43. Kraken makes many claims regarding information security standards, to "assure" customers and potential customers: "At Kraken, we use the latest standards to encrypt all sensitive account information at both the system and data level. This means your identifying information is always hidden behind a powerful layer of security. After we encrypt your information, we follow a robust set of security procedures and controls that earned us a ISO 27001 certification."[10]

44. Kraken's website further states that, "Kraken's comprehensive approach to cybersecurity and information security management systems has earned us the ISO/IEC 27001:2022 certification . . . . This demonstrates our ability to meet the highest international security standards, as well as our commitment to keeping your funds and information

[8] *FBI Private Industry Notification*, *Cyber Criminals Pose as Law Enforcement to Obtain Private User Information from U.S. Companies* 2 (Nov. 13, 2024), https://www.ic3.gov/CSA/2024/241104.pdf.

[9] Brian Krebs, *FBI: Spike in Hacked Police Emails, Fake Subpoenas*, KREBS ON SECURITY (Oct. 31, 2024), https://krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/.

[10] *How Kraken Manages Client Security*, Kraken Blog (Apr. 5, 2023), https://blog.kraken.com/crypto-education/security-at-kraken

safe."[11]

45. Kraken's representations about their cybersecurity and information security management are materially false. ISO 27001:2022 requires organizations to implement documented, risk-based access control, identity verification, and third-party management processes designed to prevent unauthorized disclosure of information. SOC 2 Type 2 requires that such controls be designed and operate effectively and consistently over an extended audit period. Kraken's disclosure of Plaintiff's personal data based solely on email domain appearance, without independent verification, out-of-band confirmation, or legal review, failed to satisfy these fundamental control requirements under both standards.[12]

46. Kraken claims its certifications "demonstrate[its] ability to meet the highest international security standards, as well as our commitment to keeping your funds and information safe."[13]

47. Kraken even brags about being steps ahead of organized crime syndicates. Its CSO Nick Percoco has stated in press interviews: "As an exchange, we're also unique in having a group of highly-skilled developers whose sole job is to attack Kraken, every single day, just like a nation state adversary or organized crime group would, to find creative ways to circumvent our controls."[14]

48. ISO/IEC 27001:2022 Annex A Controls 5.31, 5.34, 5.15, 5.16, 5.14, 8.12, 5.36, 5.24, and 5.26 collectively require that organizations (i) identify and comply with all

---

[11] *Cryptocurrency Security Protocols*, Kraken, https://www.kraken.com/features/security (last visited Jan. 30, 2026).

[12] *See Industry-leading Security Protects Your Investments, Kraken,* https://www.kraken.com/features/security (describing Kraken's ISO/IEC 27001 certification and completion of a SOC 2, Type 1 examination); *Kraken Completes SOC 2 Type 2 Compliance Report, Underscoring Commitment to Institutional Security*, Kraken Blog (June 3, 2025), https://blog.kraken.com/product/security/soc-2-type-2 (announcing completion of a SOC 2 Type 2 compliance examination for Kraken's institutional custody platform)

[13] *Id*.

[14] Michael Hill, *Interview: Nick Percoco, Chief Security Officer, Kraken*, Infosecurity Magazine (Feb. 9, 2021), https://www.infosecurity-magazine.com/interviews/interview-nick-percoco-kraken/.

applicable legal, statutory, and regulatory obligations affecting information security; (ii) protect personal data in accordance with documented policies; (iii) establish and enforce documented rules governing access to information based on defined authorization criteria; (iv) maintain the security of all information transferred internally or to external parties through documented transfer policies and protective controls commensurate with the classification of the information; (v) implement data leakage prevention tools and controls proactively designed to detect and block unauthorized transmission or disclosure of protected information; (vi) establish and enforce information security policies and procedures across all organizational processes; (vii) plan and prepare for information security incident management through defined pre-incident roles, responsibilities, and procedures; and (viii) respond to detected security incidents through a documented response program capable of containing, remediating, and communicating the incident. Kraken failed to meet each of these controls.

49. ISO/IEC 27001:2022 Annex A Control 5.31 (*Legal, Statutory, Regulatory and Contractual Requirements*) requires certified organizations to identify, document, and comply with all legal obligations related to information security, including the implementation of procedures ensuring that any disclosure of customer data is made only pursuant to a valid legal authority. This includes applicable laws that require valid legal process before disclosure, such as lawfully issued subpoenas, warrants, or court orders. This control requires that such procedures be formally documented and actively enforced, not improvised. Kraken's disclosure of Plaintiff's sensitive personal information in response to an unauthenticated email, without any verified legal instrument, effective counsel review, or confirmation of the requesting party's legal authority, directly violated Control 5.31.

50. ISO/IEC 27001:2022 Annex A Control 5.34 (*Privacy and Protection of Personally Identifiable Information*) requires certified organizations to implement and enforce documented safeguards governing when and how personal data may be disclosed to third parties, mandating both a lawful basis for disclosure and the application of protective measures commensurate with the sensitivity of the information involved.

Plaintiff's private and personal information that was exploitable for physical targeting are among the most sensitive categories of PII a financial services organization can hold. Kraken's disclosure of that information without establishing a lawful basis, verifying the requesting party's identity, or applying any documented protective measure constituted a direct violation of Control 5.34.

51. ISO/IEC 27001:2022 Annex A Control 5.14 (*Information Transfer*) requires certified organizations to establish and document rules, procedures, and contracts to maintain data security whenever information is shared internally or transmitted to external parties. The control mandates a topic-specific data transfer policy that provides information in transit with a level of protection proportional to its classification and sensitivity; requires tracking chain of custody throughout any transfer; and requires that applicable laws, regulations, and obligations be examined before any transfer occurs. Kraken's transmission of Plaintiff's sensitive personal data to an unverified external party without an assessment of whether the recipient was a legally authorized recipient constitutes a violation of Control 5.14.

52. ISO/IEC 27001:2022 Annex A Control 5.15 (*Access Control*) requires certified organizations to establish and enforce documented rules governing access to information and that access protected data be evaluated against verified identity and a legitimate, documented business need. The control requires not only that access rules exist on paper, but that they be operationally enforced at the point of every access decision. Kraken's disclosure of Plaintiff's personal data without authenticating the requesting party's identity, without a documented determination of legitimate need, and without an apparent access rule capable of preventing transmission to an unverified recipient constituted a direct violation of Control 5.15.

53. ISO/IEC 27001:2022 Annex A Control 5.24 (*Information Security Incident Management Planning and Preparation*) requires certified organizations to plan and prepare for information security incident management by establishing defined roles, responsibilities, and procedures that will govern the detection, evaluation, and initial

response to security events before an incident occurs. This control functions as the predicate to any effective incident response capability: an organization that has not planned and prepared for incident management cannot execute a meaningful response when an incident materializes. Kraken's failure to detect, evaluate, or take any apparent documented initial response to the unauthorized disclosure of Plaintiff's personal data in any timely or structured way demonstrates that Kraken lacked a functioning incident management planning program under Control 5.24.

54. ISO/IEC 27001:2022 Annex A Control 5.26 (*Response to Information Security Incidents*) separately requires certified organizations to respond to detected security incidents pursuant to a documented response procedure capable of containing, remediating, and communicating the incident as appropriate. This control requires not only a policy on paper, but an operationally active response capability that can be triggered upon detection of a security event. Kraken's months-long failure to take any documented corrective action following the unauthorized disclosure of Plaintiff's personal data demonstrates that no functioning incident response program under Control 5.26 was in place.

55. ISO/IEC 27001:2022 Annex A Control 5.36 (*Compliance with Policies, Rules and Standards for Information Security*) requires certified organizations to ensure that their information security policies and procedures are not merely drafted and published but are actively enforced and followed by personnel across all relevant processes. Where an organization holds itself out as ISO 27001:2022 certified, this control functions as the internal enforcement mechanism for every other control in the framework. This control is violated whenever a certified organization's actual conduct departs from its own documented procedures, regardless of what those procedures say. Kraken's disclosure of Plaintiff's data in a manner inconsistent with any plausible documented access control, legal compliance, or privacy protection procedure demonstrates that Kraken's information security policies were not enforced in practice, in direct violation of Control 5.36.

56. ISO/IEC 27001:2022 Annex A Control 8.12 (*Data Leakage Prevention*) is a

control that directly addresses the unauthorized transmission, or extraction of sensitive information from systems, networks, and devices. The control requires that organizations apply data leakage prevention measures designed to detect and prevent unauthorized transfers or disclosures of sensitive information and requires that sensitive information not be transmitted outside authorized channels without appropriate controls. Kraken's failure to implement any data-loss prevention measure capable of detecting or blocking the unauthorized disclosure of Plaintiff's data to an unverified external impersonator represents a particularly direct violation of Control 8.12.

57. Complementing the ISO controls described above, the AICPA 2017 Trust Services Criteria establish parallel and independently operative obligations that Kraken's SOC 2 Type 2 attestation required it to satisfy. Common Criteria CC6.1, CC6.2, and CC6.7 impose logical access, credentialing, and transmission controls; Confidentiality Criterion C1.1 requires identification and maintenance of confidential information; Common Criterion CC7.3 requires evaluation of security events and action to prevent failures; Common Criterion CC7.4 requires execution of a defined incident response program; and to the extent Kraken's SOC 2 Type 2 attestation included the Privacy category (where Kraken has implied to customers that it has), Privacy Criteria P6.1, P6.3, P6.4, and P6.6 govern disclosure consent, unauthorized disclosure recordkeeping, third-party privacy commitments, and breach notification, respectively. Kraken failed to meet each of these standards.

58. A SOC 2 Type 2 attestation is not a marketing claim or an aspiration. Rather, it is a formal declaration governed by the American Institute of Certified Public Accountants, comprising two distinct attested components: a management assertion, in which Kraken's own executives formally declared in writing that the described controls were suitably designed and operating effectively; and an independent auditor's opinion, issued by a licensed CPA firm that, based on information presented by Kraken, independently tested those controls against real-world activity across a defined audit period of six to twelve months.

59. Kraken's SOC 2 Type 2 attestation represents that the controls were not merely designed but *operating effectively and consistently* over an extended audit period and imposed parallel disclosure obligations to those mentioned above. Kraken failed to meet these requirements during the period the company's executive management had affirmatively stated in writing and attested its controls were operating effectively.

60. Common Criterion CC6.1 requires that the entity implement logical access security software, infrastructure, and architectures over protected information assets to protect them from security events, including by identifying and authenticating all persons prior to accessing information assets, whether locally or remotely, and by ensuring that new external users are registered, authorized, and documented prior to being granted access credentials. Common Criterion CC6.2 separately requires that, *prior to* issuing system credentials and granting system access, the entity register and authorize all new internal and external users, with access credentials created only upon authorization from the system's asset owner or authorized custodian. The manual disclosure of protected customer data in response to an external request is functionally equivalent to granting that external party access to protected information assets, and the same identification, authentication, and authorization safeguards apply.

61. Common Criterion CC6.7 requires that the entity restrict the *transmission, movement, and removal* of information to authorized internal and external users and processes, and that data loss prevention processes and technologies be used to restrict the ability to authorize and execute transmission, movement, and removal of information. Kraken violated all three of the aforementioned criteria: it disclosed Plaintiff's personal data to an external party whose identity was never authenticated and who had never been registered, authorized, or issued credentials under any documented approval workflow (violating CC6.1 and CC6.2); and it transmitted Plaintiff's protected personal information without any data loss prevention control capable of restricting that transmission to confirmed authorized recipients (violating CC6.7).

62. Confidentiality Criterion C1.1 requires that the entity identify and maintain

confidential information to meet its objectives related to confidentiality, including by implementing procedures to identify and designate confidential information when it is received or created and to determine the period over which it is to be retained. Kraken violated C1.1 by failing to implement or enforce procedures capable of identifying Plaintiff's data as confidential information subject to sufficient protection. This was a foundational failure that permitted the data to be disclosed to an unverified impersonator without sufficient classification-based protective measures in place.

63. Privacy Criterion P6.1 requires that personal information be disclosed to third parties only for the purposes specified in the entity's privacy notice and with the individual's consent. P6.3 required that the entity document any unauthorized disclosures and take appropriate remedial action. Kraken violated both criteria: it disclosed Plaintiff's personal information to an unverified impersonator for no purpose identified in any privacy notice and without Plaintiff's consent, in violation of P6.1; and it failed to document the unauthorized disclosure, investigate its cause, or timely notify Plaintiff that his personal information had been transmitted to an unverified third party, in violation of P6.3.

64. Privacy Criterion P6.4 requires that the entity obtain privacy commitments from vendors and other third parties who have access to personal information, and that it assess those parties' compliance on a periodic and as-needed basis, taking corrective action if necessary. Privacy Criterion P6.6 separately requires that the entity provide notification of breaches and incidents to affected data subjects, regulators, and others, and take remedial action in response to misuse of personal information. Common Criterion CC7.3 requires that the entity evaluate security events to determine whether they could or have resulted in a failure to meet the entity's objectives, and take actions to prevent or address such failures. Common Criterion CC7.4 requires that upon identification of a security incident, the entity execute a defined incident response program to *understand, contain, remediate, and communicate* the incident, including assigning roles and responsibilities, containing the incident, mitigating its ongoing effects, closing the underlying vulnerability, and developing and implementing communication protocols for

affected parties.

65. Kraken violated all four of the aforementioned controls, including P6.4, P6.6, CC7.3, and CC7.4, as evidenced by its protracted failure to detect and mitigate the security incident at issue. Kraken obtained no privacy commitments from, and performed no compliance assessment of, any party before transmitting Plaintiff's data (violating P6.4); it failed to timely notify Plaintiff, any regulator, or any other affected party that Plaintiff's personal information had been disclosed to an unauthorized impersonator (violating P6.6); it failed to evaluate the disclosure as a security event requiring organizational response (violating CC7.3); and its protracted failure to contain, remediate, or communicate the ongoing harm to Plaintiff demonstrates that no functioning incident response program under CC7.4 was in place.

66. As described herein, Kraken's material representations to its customers about its strict, industry-leading security measures and standards were false. Because Kraken failed to meet these industry standards, Kraken easily succumbed to an unsophisticated law enforcement impersonation scheme and disclosed Plaintiff's most sensitive and damaging personal information to organized criminals.

67. Taken together, these standards (ISO 27001:2022 and SOC 2) establish that any disclosure of customer information, including in response to law-enforcement or regulatory requests, must occur only pursuant to verified authority, documented procedures, and compliance with applicable legal and contractual obligations. Failure to follow these requirements by responding to an unverified, unsolicited request for customer information constitutes a failure to meet certification and audit requirements under ISO 27001:2022 and SOC 2.

68. Kraken's representations made to Plaintiff and to the world that it meets or can demonstrate compliance with ISO 27001:2022 and SOC 2 controls and standards are materially false.

Plaintiff's Account with Kraken

69. In October 2019, Plaintiff opened a cryptocurrency trading account with

Kraken using his full first and last name.

70. The representations identified above, made by Kraken to Plaintiff, were material because they concerned fundamental matters—security certifications, verification procedures, privacy protections, legal compliance, and internal controls—that reasonable customers rely upon when deciding whether to entrust personal data and assets to a cryptocurrency exchange.

71. When establishing and using his account, Plaintiff reasonably relied on Kraken's representations regarding "industry-leading" security, ISO 27001 and SOC 2 Type 2 certifications, "strict policies and procedures," "legal obligation" standards, and privacy protection commitments when deciding to be a customer with Kraken.

72. Had Plaintiff known that Defendants respond to unverified emails without court orders, without out-of-band verification, without legal review, and with deficient internal controls, Plaintiff would not have used Kraken's services or would have taken additional protective and mitigating measures.

73. Plaintiff completed Kraken's Tier 4 verification process, providing extensive personal information including his full legal name, date of birth, address, phone numbers, and identity documents.

74. After approximately five years (2019-2024), Plaintiff's portfolio was valued at approximately $10 million USD, including significant Bitcoin (BTC) and Ethereum (ETH) holdings.

75. On May 14, 2025, Kraken sent Plaintiff an email inquiring whether he was the holder of a specific high-value cryptocurrency wallet and requesting confirmation of wallet ownership. Plaintiff assumed that this was a so-called know-your-customer (KYC) request in the normal course of business for Kraken.

76. Plaintiff confirmed to Kraken that he was indeed the holder of the high-value wallet in question.

77. This May 14, 2025 email exchange demonstrates that Kraken *knew* Plaintiff was a high-value cryptocurrency holder who would be a prime target for criminal activity,

including wrench attacks, if his personal information were compromised.

78. Despite this knowledge, Kraken failed to implement security measures—let alone enhanced security measures—reasonably designed to protect Plaintiff's account and personal information.

79. Also, despite this knowledge, as described *infra*, Kraken divulged Plaintiff's most sensitive personal information to a facially defective and unlawful request for information purporting to be from law enforcement.

80. At the time Kraken did so, it knew both that Plaintiff was highly susceptible to the common wrench attacks that were occurring, and that the purveyor of the fake request for information was likely a criminal organization. Kraken ignored these facts and revealed Plaintiff's information anyway.

The Forged Italian Law Enforcement Requests

81. The Federal Bureau of Investigation has warned Kraken that criminals "gain access to US and foreign government email addresses and us[e] them to conduct fraudulent emergency data requests to US-based companies." *FBI Private Industry Notification* (Nov. 2024), https://www.ic3.gov/CSA/2024/241104.pdf. Kraken ignored that warning.

82. Between May 2025 and July 2025, the Roe Defendants sent spoofed emails purportedly from an Italian law enforcement agency, seeking information about Plaintiff for "law enforcement purposes."

83. These emails were an unsophisticated attempt to trick Kraken into divulging sensitive data, were facially defective, and obviously fake.

84. On information and belief, these spoofed emails were designed to appear as official emails from an Italian government agency, containing the logo and trademark of the Italian government, asking Kraken to disclose customer information.

85. On information and belief, the Roe Defendants sent these spoofed emails with the intent to:

a. Unlawfully obtain Plaintiff's personal identifying information and account

details;

b. Use that information to target Plaintiff for the purposes of harassment, intimidation, extortion, and kidnapping;

c. Impersonate Italian law enforcement officials and thereafter impersonate Kraken employees on the phone to Plaintiff;

d. Cause Plaintiff to fear for his safety and the safety of his family;

e. Ultimately force Plaintiff to transfer cryptocurrency through physical coercion or threats.

86. The spoofed emails contained false representations that they were authentic Italian government requests, under the auspices of the logo and trademark of an Italian agency.

87. The Roe Defendants transmitted these fake requests to Kraken electronically, by email.

88. On information and belief, the Roe Defendants used email addresses and domain names designed to appear as legitimate Italian government domains, which were in fact spoofed and not authorized by any legitimate Italian government agency.

Kraken Responds to Unlawful, Facially Defective Information Requests

89. Defendant Payward Europe Solutions Limited, an Irish-registered cryptocurrency exchange entity (company number 711781), and wholly-owned Kraken subsidiary, assists in Kraken's operations.

90. PESL established an Italian branch and secured registration as a Virtual Asset Service Provider (VASP) with Italy's *Organismo Agenti e Mediatori* (OAM) in June 2022. The OAM registration number PSV35 appears in regulatory filings and customer disclosures, confirming the branch's authorized status.

91. Under Italian criminal procedure, a request for personal data held by a business entity is legally effective to compel disclosure only if it takes the form of a valid, written, and reasoned decree (*decreto motivato*) issued by a competent judicial authority [judge or public prosecutor] and executed in accordance with statutory procedures. *See*

Art. 253(1) C.P.P. (the *autorità giudiziaria* orders seizure of the *corpus delicti* and things pertinent to the offense by *decreto motivato*); Art. 125 C.P.P. (decrees must be reasoned, *a pena di nullità* [on pain of nullity], where the law expressly requires motivation, as in Art. 253); and Art. 254-bis C.P.P. (data held by providers of IT, telematic, or telecommunications services, including traffic and location data, are acquired through a seizure ordered by the *autorità giudiziaria*). .

92. Any compulsory request for personal data under Italian criminal procedure must be embodied in a valid, written, and reasoned judicial or prosecutorial decree (*decreto motivato*), identifying the criminal proceeding and the specific information sought, and served in accordance with statutory procedures. *See* Art. 253(1) C.P.P. (seizure ordered by *decreto motivato* specifying the *corpo del reato* or things pertinent to the offense); Art. 125 C.P.P. (reasoning required, *a pena di nullità*, where the law so provides, as in Art. 253); Art. 254-bis C.P.P. (acquisition of provider-held data by the *autorità giudiziaria* through seizure ordered under Art. 253); and Art. 111, sixth paragraph, of the Italian Constitution (all judicial measures must be reasoned, reinforcing the statutory motivation requirement for measures that affect fundamental rights, including coercive evidentiary measures).

93. An unsolicited email request, standing alone, regardless of the sender's purported authority or originating domain, does not constitute lawful compulsory process under Italian law and creates no legal obligation to disclose confidential or personal data. Under the *Codice di Procedura Penale*, compulsory acquisition or production of documents or data may occur only pursuant to a formally valid order issued by the competent judicial authority in the forms prescribed by law. *See* Art. 253(1) C.P.P. (judicial seizure ordered by *decreto motivato* identifying the items to be seized and their connection to the offense); Art. 256 C.P.P. (the duty to produce documents, data, information, and computer programs arises only upon a formal request by the *autorità giudiziaria*, implemented through a *decreto di esibizione*); and Art. 125 C.P.P. (formal and motivational requirements for judicial acts where prescribed, *a pena di nullità*). In the absence of such a statutory order,

disclosure of personal data lacks the "legal obligation" basis required by Regulation (EU) 2016/679, Art. 6(1)(c), as implemented and supplemented by D.Lgs. 196/2003 (as amended), and is therefore not legally required and may be unlawful.

94. Italian authorities use established statutory procedures to serve compulsory process on foreign corporations with Italian branch establishments, including service at the branch's registered address, on its legal representative, or via certified electronic mail (*Posta Elettronica Certificata* or "PEC"); informal or extra-procedural requests fall outside these channels and are legally ineffective as means of effecting service. *See* Art. 145 C.P.C. (*Codice di Procedura Civile*) (service on legal entities is effected at the registered office or on the legal representative, and, where permitted, via telematic channels)[15]; D.L. 18 ottobre 2012, n. 179, Art. 16 and related provisions (general framework for court communications and notifications by PEC, including to and by judicial officers); and D.L. 179/2012, Art. 6-bis (establishing the INI-PEC national index of PEC addresses for enterprises and professionals, enabling lookup of any registered entity's certified address for notifications).

95. According to Italy's official certified email registry, INI-PEC (Indice Nazionale degli Indirizzi di Posta Elettronica Certificata), the PEC designated for legal service and official communications for Payward Europe Solutions Limited's Italian branch (Kraken) is peslitaly@legalmail.it.

96. Notwithstanding the foregoing, Kraken has a written policy of receiving law enforcement requests via email at lawenforcement@kraken.com.

97. Between May 2025 and July 19, 2025, Kraken received at least three (3) admittedly fake emails, characterized as law enforcement requests, from the Roe Defendants purporting to be from an Italian governmental agency. Kraken did not verify these fake emails, leaked Plaintiff's information in response, and did not notify Plaintiff that it had leaked his information until August 28, 2025.

98. According to Kraken's in-house counsel, Kraken disclosed Plaintiff's

[15] Note that this is civil law authority, not criminal.

sensitive personal data, including his name, date of birth, address, and account details, in response to what Defendants describe only as an "information request" from "the official domain (interno.it) of an Italian law enforcement agency." Defendants' counsel cited no accompanying Italian court order, magistrate authorization, or judicial process.[16]

99. "Interno.it" refers to the domain of the Italian Ministry of the Interior (Ministero dell'Interno), which is a political-administrative ministry and not itself a judicial authority or investigative police unit.

100. An email request sent from a generic "@interno.it" address is not a logical or credible vehicle for a lawful Italian compulsory request for information to a foreign cryptocurrency exchange like Kraken because it bypasses the judicial authorities and specialized investigative bodies that handle financial and cyber investigations, and it does not satisfy the formal decree and service requirements imposed by the C.P.P.

101. Emails from a generic "@interno.it" address may reflect operational or liaison communications in the context of police or international cybercrime cooperation, but they do not, by themselves, constitute compulsory legal process under Italian law absent a valid *decreto motivato* or other formal judicial act issued by the competent *autorità giudiziaria* and executed in compliance with the C.P.P.

102. An email originating from a generic "@interno.it" address may relate to high-level policy coordination, treaty-based or operational police cooperation, voluntary liaison, or referral to competent investigative bodies, but not to compulsory, case-specific demands for customer data, which under Italian law require a judicial or prosecutorial decree pursuant to Articles 253 and 254-bis C.P.P. and, where international cooperation is involved, routing through the Ministry of Justice as central authority under Articles 723 and 727 C.P.P.

103. In Italy, financial and tax investigations are primarily conducted by the *Guardia di Finanza*, a police force under the Ministry of Economy and Finance, pursuant

[16] Kraken withheld from Plaintiff that it had leaked his personal information to the criminals until August 28, 2025, after which counsel for Plaintiff and Kraken in-house counsel met and conferred to discuss this issue.

to Law 23 April 1959, n. 189 and D.Lgs. 19 March 2001, n. 68, which define it as a police force with general competence in economic and financial matters. Cyber and online investigations are handled operationally by the *Polizia Postale e delle Comunicazioni*, a specialized branch of the State Police (*Polizia di Stato*) organized within the public security department under Law 1 April 1981, n. 121 and implementing decrees. International evidence requests, including requests for customer data from foreign providers, are coordinated through the Ministry of Justice acting as central authority (*see* Council of Europe, *Italy National Procedures for Mutual Assistance in Criminal Matters* (May 3, 2021)),[17] which entrust the Minister of Justice with receiving, assessing, and transmitting incoming and outgoing requests for mutual legal assistance.

104. A bare request for Plaintiff's identifying information sent from an "@interno.it" account, unconnected to any identified investigative unit or judicial authority and unaccompanied by formal process, therefore, did not resemble a legitimate Italian compulsory legal request for account data.

105. On information and belief, Kraken responded to these fake emails sent to its non-PEC Kraken email address (@kraken.com), rather than through its official certified electronic mail PEC address. Thus, the emails from Roe Defendants, even if they were not fake and had contained actual judicial orders, would not have been legally effective requests under Italian law, which channels formal service and certified communications for companies through their registered PEC or other codified methods of service.

106. Kraken's counsel admitted that beginning August 1, 2025, Kraken's policies changed with how it responded to law enforcement requests, by requiring an Irish court order before requests would be honored.

107. When a subsequent request from the same Italian domain arrived in August 2025, Kraken informed the requester that "any request for account data must be supported by an Irish court order directed at the Irish entity."

108. The August 2025 request attached a document purporting to be an Irish court

[17] https://rm.coe.int/italy-country-information-template-mla/1680a2addf).%22%5B1

order. Kraken reviewed the document, contacted the Irish court, determined the purported court order was forged, and only then did Kraken reject the request.

109. Kraken implemented its court order requirement only after receiving a fraudulent court order in August 2025, and not because of any change in applicable law that would not have required it in the first place. Alternatively, Kraken had the ability to spot forged court orders in August, which Kraken did not implement earlier in July.

110. Had Kraken applied the same standard to the July 2025 requests, Kraken would have spotted the forged order and/or demanded a legitimate court order, and the July requests would have been rejected.

111. Moreover, since Kraken did not receive requests through its PEC designated for legal service and official communications for Payward Europe Solutions Limited's Italian branch (Kraken) at peslitaly@legalmail.it, none of the purported Italian requests were ever valid compulsory requests under Italian law.

112. Kraken was aware of at least a high probability that the purported governmental requests from the fake emails were, in fact, fraudulent attempts to steal customer information. Kraken was aware that the target of this scheme was Plaintiff, who was a customer with substantial cryptocurrency holdings and therefore susceptible to so-called wrench attacks.

113. Notwithstanding the foregoing, Kraken deliberately failed to learn the truth about the fake emails, which would have required minimal effort (basic compliance with law enforcement request norms and industry standards). Rather than take the most basic, elemental steps required to verify the emails were fake, Kraken stuck its proverbial head in the sand to ignore the fraud it knew was occurring.

114. Kraken acted with willful blindness to the scheme to steal Plaintiff's information.

115. The July and August requests originated from the same domain but received differential treatment by Kraken, where Kraken responded to some without requiring actual judicial process, but without conducting competent verification of any.

116. Kraken's law enforcement request process failed because the company prioritized cost savings measures over consumer safety.

117. The information released by Kraken in response to the spoofed email(s) included, but was not limited to, the following:

a. Plaintiff's full legal name and date of birth;

b. Plaintiff's complete address;

c. Plaintiff's phone numbers;

d. Plaintiff's account details, including his account username;

e. Financial information confirming Plaintiff's high-value account status and substantial cryptocurrency holdings;

f. Additional personal identifying information, including details of Plaintiff's business entities.

118. The above information was not available to the Roe Defendants absent Kraken's unlawful production.

119. Kraken failed to take any of the following basic verification steps before releasing Plaintiff's information:

a. Treating release of Plaintiff's account data with higher scrutiny given the proliferation of wrench attacks targeting high-value account holders;

b. Requiring actual court orders to accompany requests;

c. Verifying the authenticity of email purportedly from government agencies;

d. Contacting the purported issuing agency to confirm the legitimacy of the requests;

e. Requiring indicia of the appropriate level of security for a law enforcement agency, such as providing a link in an email back to the website of the law enforcement agency for the actual request;

f. Examining the email domains for signs of spoofing or fraud;

g. Comparing the requests to known fraudulent patterns;

h. Implementing any meaningful authentication protocol;

i. Requiring encrypted or secure transmission channels;

j. Consulting with legal counsel regarding suspicious requests;

k. Implementing enhanced verification for high-value account holders like Plaintiff.

l. Periodic and risk-based auditing or independent review of Kraken's law enforcement response program prior to continuation of the status quo processes and practices.

The Criminal Attack on July 19, 2025

120. The attacks against Plaintiff began prior to Kraken disclosing to Plaintiff that his personal information had been given to the criminal Roes.

121. On July 19, 2025, at approximately 11:44 PM, Plaintiff received a phone call from an individual identifying himself as "Daniel Li," purporting to be from Kraken's security department. "Daniel Li" was not from Kraken's security department. In fact, he was impersonating Kraken security and acting on behalf of the Roe Defendants.

122. The phone call originated from a United States phone number: +1-888-600-0173.

123. During this approximately 30-minute call, "Daniel Li" demonstrated complete and detailed knowledge of Plaintiff's personal information that could only have been obtained from Kraken's databases, including:

a. Plaintiff's full date of birth;

b. Plaintiff's complete address;

c. Plaintiff's Kraken account username;

d. Details of alleged hacking attempts on Plaintiff's account;

e. Knowledge of Plaintiff's current location and travel status.

124. This phone call was how Plaintiff first discovered that his personal information had been compromised—not through any notification from Kraken, which would not come until 39 days later.

125. "Daniel Li" claimed that Plaintiff's account had been subject to hacking

attempts from Puerto Rico, including attempts to change the email address and two-factor authentication settings.

126. "Daniel Li" requested that Plaintiff confirm personal details. When Plaintiff provided only partial information (such as his birth month instead of his full birthday), "Daniel Li" completed the information with specific details (the date and year of Plaintiff's birth), demonstrating that he already possessed this information from Kraken's disclosure.

127. Similarly, when Plaintiff provided only the street name of his address, "Daniel Li" completed it with the street number, city, and zip code, again demonstrating detailed knowledge obtained from Kraken.

128. During the call, "Daniel Li" made explicit references to physical violence and wrench attacks, stating:

a. "we don't want you getting whacked over the head with a 5 dollar wrench"

b. "I guess you are using a hardware wallet, but that is not enough, they could beat the seedphrase out of you"[18]

129. These statements were not warnings—they were threats thinly disguised as warnings. By describing what "the hackers" might do, "Daniel Li" revealed his own criminal organization's actual intentions (a psychological phenomenon known as "criminal projection").

130. "Daniel Li" attempted to induce Plaintiff to download malware by directing him to visit a fraudulent website at "pt-kraken.com" (a Portuguese-language phishing site mimicking Kraken's legitimate domain).

131. After receiving this phone call from "Daniel Li," Plaintiff attempted to open tickets with Kraken's support system—the only way Plaintiff could contact Kraken—to

[18] Roe Defendants knew, based on the blockchain information provided from Kraken, that Plaintiff had moved substantial cryptocurrency funds off of Kraken's exchange and onto hardware wallets. A hardware cryptocurrency wallet is a physical device that stores a user's private keys offline, requiring manual confirmation on the device itself before any transaction can be authorized, thereby protecting digital assets from online hacking and unauthorized access. Plaintiff did indeed have hardware wallets holding substantial funds originating from Kraken, which were purchased without providing his personal information to any retailer or anonymously with cash.

inquire about the security of his account and his personal information. Plaintiff received no response from Kraken.

132. After Kraken ignored Plaintiff's ticket requests, Plaintiff emailed Kraken to inquire about the status of his open tickets. Plaintiff received an automatic response that he would be required to submit *another* support ticket to ask about the status of his first request.

133. By this time, Plaintiff felt completely abandoned by Kraken, and the fear for his personal and family safety began to heighten. Plaintiff was aware, like most everyone connected to the cryptocurrency industry that pays attention to the news, that targeted violent wrench attacks were being perpetrated on an alarming scale against high-net-worth cryptocurrency consumers.

134. Roe Defendants displayed they had unfettered access to Plaintiff's personal information, and fearing that his communications with Kraken were also being intercepted by the Roe Defendants, Plaintiff attempted to *close* his open tickets. He was unable to do so.

135. By this point, on July 20, 2025, when Plaintiff contacted Kraken by email and through support tickets to report the security incident immediately after receiving the call from "Daniel Li," it is beyond dispute that Kraken was aware that Plaintiff's data had been compromised.

136. Kraken ignored Plaintiff's pleas for help.

Plaintiff's Flight and the Coordinated Surveillance Operation

137. Within 24 hours of the July 19, 2025, criminal contact, Plaintiff made the emergency decision to flee for his safety.

138. For the next ten (10) days (July 20-30, 2025), Plaintiff was forced to hide alone, driving around a foreign nation where he was on a business trip, having just completed the sale of a property, and changing hotels every 1-2 nights to avoid being tracked.

139. Plaintiff has lived in constant fear of being followed and was afraid to return

to his country, as flight manifests could reveal his location and his address could be easily discovered online.

140. Plaintiff's fear has been reasonable and based on specific, articulable events that occurred, showing the Roe Defendants have targeted Plaintiff following the Kraken information leak.

141. During this period, Plaintiff received multiple suspicious phone calls from various international numbers from different continents, indicating ongoing surveillance and attempted contact by the criminal organization.

142. On July 30, 2025, Plaintiff fled, by plane, the country where he had been hiding, to a series of intermediate destinations before ultimately reaching a secure location maintained by family members whose address is not publicly associated with Plaintiff.

143. While Plaintiff was in hiding, on or about August 5, 2025, the Roe Defendants conducted a coordinated multi-person surveillance operation at Plaintiff's apartment.

144. Specifically, an unknown individual gained unauthorized access to Plaintiff's apartment building and attempted to force entry into Plaintiff's apartment on the second floor.

145. The individual rang the doorbell repeatedly and then engaged in loud, aggressive banging on the door.

146. A friend of Plaintiff who was at the apartment collecting belongings at Plaintiff's request, was inside at the time and heard the attempted entry. He did not open the door and remained silent until the intruder left.

147. Immediately after leaving the building, Plaintiff's friend was approached by a man in his mid-50s who interrogated him about the apartment, asking:

a. Whether the friend was renting the apartment on the second floor;

b. Whether Plaintiff was "still around in [the city where Plaintiff's apartment is located]"; and

c. What the friend did for work.

//

Kraken's Unconscionable 39-Day Delay in Notification

148. Despite having discovered by July 19, 2025, at the latest, that it had released customer information in response to fake government requests, Kraken did not notify Plaintiff of the breach until August 28, 2025.

149. Kraken has provided no explanation why it took the company 39 days to inform Plaintiff.

150. This 39-day delay meant that Kraken's notification came:

a. After criminals had already used the data to attack Plaintiff;

b. After Plaintiff had already spent 10 days fleeing in terror by car and then fled the country by flight;

c. After criminals had already conducted surveillance at Plaintiff's apartment;

d. After the criminal organization had already completed its reconnaissance and intelligence gathering.

151. When Kraken finally sent Plaintiff a breach notification on August 28, 2025, Kraken's email downplayed the severity of the breach.

152. Kraken explained how they caught a "forged court order" and did not respond to it, glossing over how they received previous request(s) *just by email* to which they responded with Plaintiff's personal information:

> "While this request [the forged court order] was identified and rejected, we also found two earlier [email] requests from the same domain that Kraken, acting in good faith and in line with our legal obligations, had responded to."

153. The phrase "acting in good faith" is misleading and false. Kraken acted in willful and reckless disregard for Plaintiff's safety. In the best light, Kraken was grossly negligent and in breach of its duties by releasing information in response to unverified, facially defective email(s), not official legal process, particularly regarding a known high-value account holder who Kraken knew was susceptible to a wrench attack.

154. The notification further stated:

> "The data potentially affected may include: Contact information, such as name and address"

155. It is critical to understand that Kraken *knew* that Plaintiff's information had

been obtained by criminals using a *modus operandi* that was significantly associated by Kraken with violent wrench attacks.

156. Despite this knowledge, Kraken attempted to minimize the severity of the breach by failing to emphasize that:

a. The criminals obtained a complete personal profile enabling physical targeting;

b. Plaintiff was a confirmed high-value target;

c. Plaintiff should take extreme precautions to protect his and his family's personal safety.

157. The notification assured Plaintiff that his "assets remain safe," completely missing the point that Plaintiff was in danger of physical attack and kidnapping, not a mere account takeover.

158. Kraken's 39-day delay violated:

a. California's data breach notification law (California Civil Code §1798.82), which requires notification "in the most expedient time possible and without unreasonable delay"; and

b. Industry best practices for immediate notification of high-risk customers.

159. This delay was particularly unconscionable because Kraken knew as of May 14, 2025, that Plaintiff was a high-value target who faced heightened risk if his information were compromised.

Harm to Plaintiff and His Family

160. As a direct and proximate result of Defendants' unlawful conduct, Plaintiff and his family have suffered irreparable harm.

Forced Displacement

161. Plaintiff cannot safely return to his apartment or to any other previously known address.

162. Plaintiff's family had to temporarily separate. Plaintiff had to temporarily separate from his wife and children, because the security threat has made it untenable for

them to stay together.

163. Plaintiff was forced to abandon his apartments due to the security compromise. Because the breach revealed Plaintiff's connections in multiple locations (through publicly traceable corporate and family records), Plaintiff has been systematically cut off from multiple locations where he has ties. These locations have become high-risk environments for Plaintiff.

Danger to Minor Children

164. Plaintiff has two minor children whose names directly link them to their father's identity and cryptocurrency holdings.

165. Plaintiff's minor children face heightened risk because their identities are connected to Plaintiff through public records, making them potential targets for criminal exploitation to coerce Plaintiff.

Business Destruction

166. Plaintiff is a successful entrepreneur. The data breach has significantly harmed his ability to do business.

167. The harm to Plaintiff's business ventures has resulted in estimated losses in the millions of dollars.

Severe Psychological Trauma

168. As a result of Defendants' actions, Plaintiff suffers from severe emotional distress and anxiety, manifesting in physical and psychological symptoms.

169. Plaintiff requires ongoing treatment and medication to manage the effects of the breach and ongoing threats.

170. Plaintiff's wife and children also suffer severe emotional distress from the constant security threat.

Security Costs

171. Plaintiff and his family require extensive security measures for the foreseeable future, including: home security systems and relocation and immigration costs necessitated by the ongoing security threat, among other costs.

172. Plaintiff has already spent significant amounts on security in attempts to keep himself and his family safe from the Roe Defendants and their cohorts.

173. These security costs are significant for Plaintiff alone.

Law Enforcement Filings and Ongoing Threat

174. Within 48 hours of receiving Kraken's belated breach notification, Plaintiff filed formal criminal complaints with law enforcement authorities in three countries.

175. Plaintiff also prepared filings for Interpol requesting Yellow, Purple, and Green Notices regarding the international criminal organization.

176. Active criminal investigations are ongoing in all three jurisdictions.

177. The criminal threat has not ceased. On October 28, 2025—more than three months after the initial July attack—criminals contacted Plaintiff again regarding his Kraken account. Additionally, Plaintiff has detected unauthorized login attempts on his other cryptocurrency exchange accounts originating from international IP addresses, including from Russia. These incidents demonstrate that the threat remains active, ongoing, and escalating, and that the criminal organization continues to exploit the breached data across multiple platforms.

178. Kraken has not offered any support to Plaintiff, and has shared no significant information with Plaintiff to aid in his law enforcement investigations or to protect his family.

FIRST CAUSE OF ACTION

Doxing in Violation of California Civil Code §1708.89

(Against Roe Defendants)

179. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

180. California Civil Code §1708.89 creates a private right of action against any person who, with intent to place another person in reasonable fear for their safety, or the safety of the other person's immediate family: 1) by means of an electronic communication device, 2) without the consent of the other person, 3) for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party, 4)

electronically distributes, publishes, emails, hyperlinks, or makes available for downloading, personally identifying information, 5) where the distribution of such information would be likely to incite or produce that unlawful action.

181. The Roe Defendants obtained Plaintiff's personal identifying information, including his full legal name, date of birth, address, account username, and confirmation of his high-value cryptocurrency holdings, through fraud and fake Italian law enforcement requests.

182. The Roe Defendants intentionally used, shared, and disseminated this information within their criminal organization and with third parties, on information and belief via electronic communications devices (telephones, cell phones, computers, webpages, or websites, etc.) for the purpose of surveilling Plaintiff, attempting forced entry at his apartment, threatening him with "wrench attacks," and preparing a kidnapping and extortion scheme.

183. The Roe Defendants knew and intended that the disclosure and use of Plaintiff's information, within their criminal organization and with third parties, would place Plaintiff and his family in reasonable fear for their safety and would cause severe emotional distress, disruption of their lives, and economic harm.

184. As a direct and proximate result of the Roe Defendants' doxing, Plaintiff suffered catastrophic harm including forced location moves, forced abandonment of his apartment, harm to business opportunities, danger to his minor children, wife, and extended family, severe psychological trauma, and ongoing security costs.

185. Plaintiff is entitled to recover: (a) general and special damages according to proof; (b) statutory damages of not less than $1,500 and not more than $30,000 per violation pursuant to California Civil Code 1708.89(c); (c) punitive damages pursuant to Civil Code 3294; (d) reasonable attorney's fees pursuant to Civil Code §1708.89(d); and (e) costs of suit.

//

//

SECOND CAUSE OF ACTION

Aiding and Abetting Doxing in Violation of California Civil Code §1708.89

(Against Kraken Defendants)

186. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

187. The Roe Defendants' conduct constitutes doxing in violation of California Civil Code §1708.89.

188. The Kraken Defendants had actual knowledge, or consciously avoided such knowledge, that they were responding to fake law enforcement requests designed to obtain Plaintiff's personal identifying information for unlawful purposes, including harassment, extortion, and physical harm.

189. Despite this knowledge, Kraken released Plaintiff's complete personal identifying information and account details in response to Roe Defendants' fake legal request, without undertaking basic verification steps such as confirming the authenticity of the purported requests, checking the email domains, or consulting legal counsel.

190. Kraken's willful blindness in responding to the Roe Defendants' fake law enforcement requests substantially assisted and enabled the Roe Defendants' doxing, without which the criminal organization could not have credibly impersonated Italian law enforcement and Kraken itself, targeted Plaintiff, or executed the reconnaissance, surveillance, and attempted forced entry operations.

191. As a direct and proximate result of Kraken's substantial assistance, Plaintiff suffered the severe harm described above and is entitled to general and special damages, statutory damages, punitive damages, attorney's fees, and costs.

THIRD CAUSE OF ACTION

Breach of Fiduciary Duty

(Against Kraken Defendants)

192. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

193. A confidential or fiduciary relationship existed between Plaintiff and Kraken arising from: (a) Kraken's custody and control over Plaintiff's sensitive personal information and high-value cryptocurrency assets; (b) Plaintiff's necessary reliance on and trust in Kraken to safeguard such information and assets; (c) Plaintiff's vulnerability to misuse of that information; and (d) Kraken's superior knowledge and expertise regarding cryptocurrency security risks and data protection obligations, which created a relationship of trust and confidence.

194. Based on the confidential relationship described above, Kraken owed Plaintiff fiduciary duties including: (a) the duty of utmost care in safeguarding Plaintiff's personal data and cryptocurrency assets; (b) the duty of loyalty to act in Plaintiff's best interests rather than Kraken's own convenience; (c) the duty of full and fair disclosure regarding security breaches and risks to Plaintiff's information; and (d) the duty to avoid conflicts of interest between Kraken's business interests and Plaintiff's security needs.

195. Kraken breached these fiduciary duties by, among other things: (a) disclosing Plaintiff's data in response to fake law enforcement email requests without verification; (b) failing to implement enhanced protections for a known high-value account holder; (c) delaying breach notification for 39 days; and (d) materially downplaying the severity of the breach in its August 28, 2025 email.

196. As a direct and proximate result of Kraken's breaches of fiduciary duty, Plaintiff suffered catastrophic economic, emotional, and security-related harms and is entitled to compensatory and punitive damages, as well as equitable relief.

FOURTH CAUSE OF ACTION

Misrepresentation

(Against Kraken Defendants)

197. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

198. Kraken made material representations in its public statements, press documents, and security materials that it holds customers' cryptocurrency safe and, above

all, it protects its customers' personal and private information, including against organized crime and security risks unique to customers operating on a cryptocurrency exchange.

199. These representations were false or misleading because Kraken in fact released Plaintiff's information without verifying obviously suspicious alleged foreign legal process and failed to timely notify Plaintiff once the breach was discovered.

200. Kraken knew, or recklessly disregarded the fact, that these statements were false when made, and intended that customers like Plaintiff would rely on them in deciding to open and maintain high-value accounts with Kraken.

201. Plaintiff reasonably relied on Kraken's representations about security and verification practices in choosing to use Kraken and to keep substantial cryptocurrency holdings on the platform.

202. As a direct and proximate result of this reliance, Plaintiff suffered the harms described above and is entitled to damages, including punitive damages for Kraken's fraudulent conduct.

FIFTH CAUSE OF ACTION

Breach of Contract

(Against Kraken Defendants)

203. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

204. Plaintiff and Kraken entered into valid and enforceable contracts, including the Terms of Service and Privacy Policy in effect when Plaintiff opened his account in October 2019.

205. These contracts obligated Kraken to implement reasonable security measures, protect personal customer information from unauthorized disclosure, and comply with applicable data-protection and notification laws.

206. Among other things, Section 3.2 of Kraken's Terms of Service required Plaintiff to maintain the security of his Kraken Account and promptly notify Kraken of any suspected breach—which Plaintiff did. Meanwhile, Kraken retained custody of his "Funds"

within a “Kraken Account” that Kraken stored “on behalf of a user,” i.e., Plaintiff. Kraken thereby undertook corresponding obligations to operate secure systems and controls over Plaintiff’s customer account and associated identifying information.

207. Section 4 of the Terms of Service expressly incorporates Kraken’s Privacy Policy—”for information about how we collect, use and share your information”—thereby binding Kraken to its contractual promises regarding the collection, protection, use, and disclosure of Plaintiff’s personal data and its compliance with applicable data-protection and breach-notification laws.

208. The Eligibility and Acceptable Use provisions further condition use of Kraken’s services on compliance with applicable law and prohibit conduct that would “cause damage to [Kraken’s] services or systems.” This provision reinforces that Kraken’s own performance of the contract—including its handling and disclosure of customer information—would conform to applicable data-protection and notification statutes such as California Civil Code §1798.82.

209. Kraken breached these contractual obligations by disclosing Plaintiff’s information to forged law enforcement requests without verification and by failing to notify Plaintiff of the breach “in the most expedient time possible and without unreasonable delay.”

210. As a direct and proximate result of Kraken’s breaches, Plaintiff sustained substantial damages, including the economic, emotional, and security-related losses described herein, and is entitled to recover such damages according to proof at trial.

SIXTH CAUSE OF ACTION

Breach of Implied Covenant of Good Faith and Fair Dealing

(Against Kraken Defendants)

211. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

212. Every contract between Plaintiff and Kraken, including the Terms of Service and Privacy Policy, contained an implied covenant of good faith and fair dealing prohibiting

Kraken from acting in a manner that unfairly frustrated Plaintiff's rights to the benefits of the contracts.

213. Kraken breached the implied covenant by: (a) releasing Plaintiff's data to criminals despite knowing he was a high-value target; (b) prioritizing its own convenience and liability management over Plaintiff's safety; (c) delaying notification for 39 days; and (d) minimizing the scope and consequences of the breach in its communications.

214. As a direct and proximate result, Plaintiff was deprived of the contractual benefits of secure account management and data protection and suffered the extensive harms described above, entitling him to compensatory and punitive damages.

SEVENTH CAUSE OF ACTION

Unfair Competition

(California Business and Professions Code §17200)

(Against Kraken)

215. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

216. The Kraken Defendants ("Kraken") have engaged in unlawful, unfair, and fraudulent business acts and practices within the meaning of California Business and Professions Code §17200.

A. Unlawful Business Acts and Practices

217. Kraken has violated California Civil Code section 1708.89 (California's anti-doxing statute) by aiding and abetting doxing, as further alleged in Plaintiff's Second Cause of Action for Aiding and Abetting Doxing in Violation of Civil Code section 1708.89, which Plaintiff incorporates here for purposes of the "unlawful" prong of the UCL. The "unlawful" conduct includes, but is not limited to:

a. Kraken had actual knowledge, or consciously avoided such knowledge, that it was responding to fake foreign "law enforcement" requests for Plaintiff's personal identifying information designed for harassment, extortion, and physical harm, particularly in light of Kraken's May 14, 2025 confirmation that Plaintiff was a high-value

target and Kraken's own public recognition of wrench-attack risks.

b. Kraken disclosed Plaintiff's full name, date of birth, address, phone numbers, Kraken account username, and confirmation of high-value cryptocurrency holdings in response to at least one fake request, despite multiple red flags, including spoofed domains and a later-confirmed forged Irish court order.

c. Kraken substantially assisted Roe Defendants' doxing by enabling Roe Defendants to build a complete profile of Plaintiff, impersonate Kraken in the July 19, 2025 call, conduct physical surveillance, attempt forced entry at Plaintiff's apartment, and prepare a kidnapping and extortion operation.

218. Kraken has violated California Civil Code section 1798.82 (data-breach notification) by failing to timely and adequately notify Plaintiff of the breach. This same notification failure supports Plaintiff's Fifteenth Cause of Action for Fraudulent Concealment and related data-breach allegations, which Plaintiff incorporates here as predicate "unlawful" acts. The conduct includes, but is not limited to:

a. Kraken discovered, at the latest by July 19, 2025, that it had released customer information in response to fake law enforcement requests, as shown by the July 19, 2025 attack on Plaintiff and Kraken's subsequent internal investigation revealing multiple prior email-only requests from the same spoofed domain.

b. Kraken failed to notify Plaintiff of the breach until August 28, 2025—39 days later—despite knowing that Plaintiff was a high-value account holder and that criminals had already used the leaked data to contact him, threaten wrench-attack-type violence, and conduct surveillance at his apartment.

c. Kraken sent a notification that minimized the breach by describing affected data merely as "contact information, such as name and address," and falsely characterized earlier responses to spoofed emails as made "in good faith and in line with our legal obligations," while omitting the full scope and risk of the disclosure.

219. Kraken has violated California Business and Professions Code section 17500 et seq. (False Advertising Law), as further alleged in Plaintiff's Ninth Cause of Action

for False Advertising, which Plaintiff incorporates here as additional predicate "unlawful" conduct. The conduct includes, but is not limited to:

a. Kraken publicly represented in marketing and on its website that "security is embedded in every company decision," that Kraken is "in many respects…a security company that operates a crypto exchange," that Kraken uses "the latest standards" and "robust" procedures to protect client funds and personal information, and that Kraken maintains the "highest standards of data protection, privacy, and compliance."

b. Kraken's Chief Security Officer publicly portrayed Kraken's security culture as "far higher" than competitors and referenced "superior practices," including a dedicated internal team simulating nation-state and organized-crime attacks to stay ahead of adversaries.

c. Kraken made these statements despite responding to plainly suspicious foreign email requests without basic verification and then delaying and downplaying breach notification, thereby rendering the statements untrue or misleading as applied to Kraken's handling of Plaintiff's data.

220. Kraken has also violated California law prohibiting misrepresentation, concealment, and misappropriation of confidential information, as alleged in Plaintiff's Fourth Cause of Action (Misrepresentation), Fifteenth Cause of Action (Fraudulent Concealment), and Sixteenth Cause of Action (Misappropriation of Confidential Information), which Plaintiff incorporates here as additional predicate "unlawful" conduct. That conduct includes, but is not limited to:

a. Kraken misrepresented to Plaintiff that it had acted "in good faith and in line with our legal obligations" in responding to prior email requests, even though Kraken failed to perform basic checks such as domain verification, contacting the purported agencies, or consulting legal counsel.

b. Kraken concealed from Plaintiff, for 39 days, that Plaintiff's complete personal profile and high-value account status had been disclosed to criminals through unverified requests, despite Kraken knowing or having reason to know (based on Plaintiff's

own communications to Kraken through support tickets and emails) that Plaintiff faced an acute risk of physical harm.

c. Kraken misappropriated Plaintiff's confidential information by disclosing it to third-party criminals without authorization or legal justification, and by failing to implement enhanced safeguards commensurate with Plaintiff's known risk profile.

221. As a direct and proximate result of Kraken's unlawful business acts and practices, Plaintiff has suffered economic injury and loss of money or property, including but not limited to: abandonment of his apartment; loss of business value and business opportunities; substantial expenditures for emergency relocation and ongoing security; and other out-of-pocket losses and economic harms.

B. Fraudulent Business Acts and Practices

222. Kraken's business acts and practices are fraudulent within the meaning of the UCL because they were likely to deceive reasonable consumers, including Plaintiff, about Kraken's security practices, verification procedures, and handling of the breach.

223. Kraken's fraudulent conduct includes, but is not limited to:

a. Kraken's security marketing, website statements, and public interviews created the false impression that Kraken rigorously verified law enforcement requests, employed superior security practices, and prioritized protection of both client funds and personal identifying information, when in fact Kraken failed to implement adequate verification procedures.

b. Kraken induced Plaintiff to open and maintain a high-value account and to trust Kraken's security and breach-response processes based on these representations. Specifically, Kraken made false and fraudulent representations about its information security, falsely representing that its compliance environment met the controls and standards of SOC 2 Type 2 and ISO/IEC 27001:2022. Plaintiff reasonably relied on these representations, thereby increasing Plaintiff's vulnerability when Kraken later failed to verify requests or timely disclose the breach.

c. Kraken's August 28, 2025 breach notification omitted material facts

about the scope of information disclosed, the number and nature of prior fake requests, and the timing of Kraken's knowledge, while using "good faith" language that falsely suggested compliance with applicable legal and industry standards.

224. These fraudulent acts and omissions are the same misrepresentations and concealments alleged in Plaintiff's Fourth Cause of Action (Misrepresentation), Ninth Cause of Action (False Advertising), Fifteenth Cause of Action (Fraudulent Concealment), and any other applicable causes of action for fraudulent conduct, which Plaintiff incorporates here as predicate "fraudulent" conduct under Business and Professions Code section 17200.

C. Unfair Business Acts and Practices

225. For purposes of the UCL's "unfair" prong, Plaintiff alleges that the injury caused by Kraken's conduct is substantial, is not outweighed by any countervailing benefits to consumers or competition, and is not an injury that Plaintiff could reasonably have avoided.

226. Kraken's unfair conduct includes, but is not limited to:

a. Kraken represented to Plaintiff and the public that it maintained ISO/IEC 27001:2022 certification and SOC 2 Type 2 attestation, both of which require that customer data protection controls be not merely documented but operationally effective — representations on which Plaintiff reasonably relied in entrusting Kraken with his personal and financial information. Kraken's failure to implement any functioning access authentication, data transmission control, or incident response capability demonstrates that those representations were false, causing substantial harm to Plaintiff that he could not have reasonably avoided. This conduct offends the established public policy of California protecting consumers from unauthorized disclosure of personal data and constitutes an unfair business practice.

b. Kraken released highly sensitive personal identifying information for a known high-value account holder to unverified foreign email requesters, without performing elementary verification or implementing heightened safeguards appropriate to the known

risk of wrench attacks and kidnapping.

c. Kraken delayed notification of the breach for 39 days, even though Kraken knew or should have known (based on Plaintiff's own emails and support tickets submitted to Kraken) that Plaintiff's information had already been weaponized against him in the July 19, 2025 call, the subsequent suspicious calls, and the coordinated surveillance and attempted forced entry at Plaintiff's apartment.

d. Kraken minimized the severity of the breach in its notification and subsequent communications, mischaracterized the nature of the data disclosed, and failed to warn Plaintiff about the specific risk of physical targeting and kidnapping arising from Kraken's disclosure.

227. The injury caused by Kraken's unfair practices is substantial: Plaintiff and his family have been forced into permanent displacement, have incurred and will continue to incur significant security costs, have suffered severe emotional and psychological harm, and have experienced major business and economic losses. Any purported benefits to consumers or competition from Kraken's failure to verify law enforcement requests, delay in notification, or minimization of the breach are nonexistent or negligible and are far outweighed by the severe harms imposed on Plaintiff. Plaintiff could not reasonably have avoided these injuries because Kraken alone controlled whether and how to verify purported law enforcement requests, when and how to notify Plaintiff about data breaches, and what information to disclose about the breach.

228. Kraken's unlawful, fraudulent, and unfair business acts and practices were a substantial factor in the overall criminal scheme perpetrated against Plaintiff, and Kraken is jointly and severally liable with Roe Defendants for restitution of all money or property Plaintiff lost as a result of those practices.

229. As a direct and proximate result of Kraken's unlawful, unfair, and fraudulent business acts and practices, Plaintiff has suffered injury in fact and has lost money or property, including but not limited to: abandonment of his apartment; loss of business value and business opportunities; substantial expenditures for relocation and ongoing security;

and other out-of-pocket losses. Plaintiff therefore has standing to pursue this claim under Business and Professions Code sections 17200 and 17204 and seeks restitution, disgorgement, and injunctive relief under section 17203, including orders requiring Kraken to cease the challenged practices, implement adequate verification and security procedures, and provide corrective disclosures regarding the breach and its handling.

EIGHTH CAUSE OF ACTION

Unfair Competition

(California Business and Professions Code §17200)

(Against Roe Defendants)

230. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

231. Roe Defendants have engaged in unlawful, unfair, and fraudulent business acts and practices within the meaning of California Business and Professions Code section 17200.

A. Unlawful Business Acts and Practices

232. Roe Defendants have violated California Civil Code section 1708.89 (doxing), as alleged in Plaintiff's First Cause of Action for Doxing in Violation of Civil Code section 1708.89, which Plaintiff incorporates here as predicate "unlawful" conduct. The conduct includes, but is not limited to:

a. Roe Defendants sent spoofed emails, purporting to be from an Italian law enforcement agency, to Kraken to obtain Plaintiff's personal identifying information—including full name, date of birth, address, account username, and confirmation of high-value cryptocurrency holdings—without Plaintiff's consent.

b. Roe Defendants electronically distributed, shared, and used Plaintiff's personal identifying information within their criminal organization and with third parties to plan and execute surveillance, attempted forced entry at Plaintiff's apartment, and a kidnapping and extortion scheme.

c. Roe Defendants acted with the intent to place Plaintiff and his family in

reasonable fear for their safety and to imminently cause unwanted physical contact, injury, and harassment by third parties.

233. Roe Defendants have violated California Penal Code section 528.5 (electronic impersonation), as further alleged in Plaintiff's Tenth Cause of Action for Violation of Penal Code section 528.5, which Plaintiff incorporates here as predicate "unlawful" conduct. The conduct includes, but is not limited to:

a. Roe Defendants credibly impersonated Italian law enforcement officials in email communications to Kraken by using spoofed email addresses, spoofed domains, and the logo and trademark of an Italian law enforcement agency.

b. Roe Defendants credibly impersonated Kraken employees (including "Daniel Li" from Kraken's security department) in phone calls to Plaintiff, using detailed information obtained from Kraken's disclosure to pose as legitimate Kraken security personnel.

c. Roe Defendants knowingly undertook these impersonations without consent and for the purpose of harming, intimidating, threatening, and defrauding Plaintiff.

234. Roe Defendants have violated trademark and related laws protecting against unauthorized use of official marks. The conduct includes, but is not limited to:

a. Roe Defendants used the trademark and logo of an Italian law enforcement agency, without authorization, in spoofed emails to Kraken.

b. Roe Defendants deployed those official insignia to falsely suggest government authority and to induce Kraken to disclose Plaintiff's personal identifying information and account details.

c. Roe Defendants used the unlawfully obtained information and Kraken's branding to operate phishing websites, including "pt-kraken.com," and to lend credibility to subsequent extortionate contacts with Plaintiff.

235. As a direct and proximate result of Roe Defendants' unlawful business practices, Kraken disclosed Plaintiff's data, Roe Defendants carried out the July 19, 2025 attack, coordinated surveillance and attempted forced entry at Plaintiff's apartment, and

Plaintiff suffered forced displacement, security expenditures, business losses, and severe emotional harms.

B. Fraudulent Business Acts and Practices

236. Roe Defendants' conduct is fraudulent within the meaning of the UCL because it was designed to deceive Kraken, Plaintiff, and others, and is likely to mislead reasonable persons into believing Roe Defendants were legitimate law enforcement officials or Kraken employees.

237. Roe Defendants' fraudulent conduct includes, but is not limited to:

a. Roe Defendants created and used spoofed email domains and addresses designed to look like legitimate Italian law-enforcement domains, and attached forged legal process to their requests to Kraken.

b. Roe Defendants falsely represented themselves to Kraken as Italian law enforcement officials, and to Plaintiff as bona fide Kraken security staff in the July 19, 2025 call, using accurate personal details to enhance credibility and induce trust.

c. Roe Defendants operated fraudulent websites, including "pt-kraken.com," designed to mimic Kraken's legitimate site and trick Plaintiff into downloading malware or otherwise compromising his security.

238. Through these fraudulent acts and practices, Roe Defendants induced Kraken to disclose Plaintiff's confidential information and induced Plaintiff to engage with Roe Defendants under the mistaken belief that he was dealing with legitimate authorities or Kraken personnel, thereby facilitating Roe Defendants' extortion and kidnapping scheme. The same fraudulent scheme is alleged in Plaintiff's First and Tenth Causes of Action (including doxing and electronic impersonation), which Plaintiff incorporates here as predicate "fraudulent" conduct under Business and Professions Code section 17200.

C. Unfair Business Acts and Practices

239. For purposes of the UCL's "unfair" prong, Plaintiff alleges that the injury caused by Roe Defendants' conduct is substantial, is not outweighed by any countervailing benefits to consumers or competition, and is not an injury that Plaintiff could reasonably

have avoided.

240. Roe Defendants' unfair conduct includes, but is not limited to:

a. Roe Defendants orchestrated a criminal operation to obtain Plaintiff's personal identifying information under the guise of law-enforcement authority, then used that information to threaten wrench-attack-type violence, conduct physical surveillance, attempt forced entry at Plaintiff's apartment, and plan kidnapping and extortion.

b. Roe Defendants targeted Plaintiff's minor children as high-value kidnap victims by leveraging their knowledge of Plaintiff's identity, wealth, and family structure to maximize coercive leverage.

c. Roe Defendants forced Plaintiff and his family into permanent displacement, required substantial present and future security expenditures, destroyed or severely impaired Plaintiff's business, and caused severe psychological trauma to Plaintiff and his family.

241. Roe Defendants' conduct is substantially injurious to consumers, offends established public policy against doxing, impersonation, extortion, kidnapping, and misuse of confidential information, and is immoral, unethical, oppressive, and unscrupulous. The gravity of the harm caused to Plaintiff—including ongoing risk of kidnapping or physical harm, loss of home, destruction of business opportunities, and ongoing security burdens—far outweighs any conceivable benefit from Roe Defendants' practices. Plaintiff could not reasonably have avoided Roe Defendants' unfair practices because Roe Defendants operated covertly, misused Italian government and Kraken branding to appear legitimate, and escalated to physical surveillance and attempted forced entry, leaving Plaintiff with no reasonable option other than costly flight and security measures.

242. As a direct and proximate result of Roe Defendants' unlawful, fraudulent, and unfair business acts and practices, Plaintiff has suffered injury in fact and has lost money or property, including the losses and expenses described above. Plaintiff therefore has standing to pursue this claim under Business and Professions Code sections 17200 and 17204 and seeks restitution, disgorgement, and injunctive relief under section 17203,

including orders requiring Roe Defendants to cease their unlawful practices, disgorge all ill-gotten gains, and return or destroy Plaintiff's personal identifying information.

NINTH CAUSE OF ACTION

False Advertising

(California Business and Professions Code §17500)

(Against Kraken Defendants)

224. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

243. Kraken publicly disseminated advertising and promotional statements regarding its security, verification procedures, and protection of customer data, including statements that its security culture was "far higher" than competitors and that it maintained "superior practices."

244. These statements were untrue or misleading because Kraken released Plaintiff's information without basic verification and failed to timely notify him of the breach.

245. Kraken knew or should have known that these statements were false or misleading, yet made them with the intent that consumers, including Plaintiff, would rely on them.

246. Plaintiff was deceived and reasonably relied on Kraken's false advertising in maintaining his high-value account, and as a result suffered the harms described herein, entitling him to restitution, injunctive relief, and other remedies under California Business and Professions Code §17500 *et seq.*

TENTH CAUSE OF ACTION

Violation of California Penal Code §528.5

(Electronic Impersonation)

(Against Roe Defendants)

247. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

248. The Roe Defendants knowingly and without consent credibly impersonated

Kraken and its employees to Plaintiff through phone calls, emails, and fraudulent websites, including the website pt-kraken.com, for the purpose of harming, intimidating, threatening, and defrauding Plaintiff.

249. This credible impersonation caused Plaintiff to reasonably believe he was dealing with Kraken's security department, thereby giving him a false sense of security in sharing his identifying information with the Roe Defendants initially, then intensifying his fear after he realized he was dealing with criminal operations and *not* Kraken, and increasing his vulnerability to the criminal scheme.

250. As a result of the Roe Defendants' violation of California Penal Code §528.5, Plaintiff suffered emotional distress, economic loss, and severe security consequences and is entitled to civil remedies, including damages and injunctive relief.

251. The Roe Defendants knowingly and without consent impersonated Italian law enforcement officials through, on information and belief, phone calls, emails, and fraudulent websites for the purpose of harming, intimidating, threatening, and defrauding Plaintiff.

252. This impersonation caused Kraken to believe it was dealing with Italian law enforcement security department, causing Kraken to respond to the Roe Defendants' fake email request from Italian authorities (using without authorization the trademark and logo of the agency) and disclose Plaintiff's personal identifying information and the worth of his high-value cryptocurrency account with Kraken.

253. As a result of the Roe Defendants' violation of California Penal Code §528.5, and Kraken's reliance on Roe Defendants' impersonation and disclosure of Plaintiff's personal identifying information, Plaintiff suffered emotional distress, economic loss, and severe security consequences and is entitled to civil remedies, including damages and injunctive relief.

//

//

//

ELEVENTH CAUSE OF ACTION

Negligence

(Against Kraken Defendants)

254. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

255. Kraken owed Plaintiff a duty of reasonable care to protect his personal information, to implement and follow adequate verification procedures for legal process, and to timely notify him of any breach.

256. Kraken breached this duty by: (a) failing to investigate fake Italian law enforcement requests; (b) failing to implement enhanced security for high-value account holders; and (c) delaying breach notification for 39 days despite knowing Plaintiff faced heightened risk.

257. It was reasonably foreseeable that releasing Plaintiff's data without verification would expose him to criminal targeting, physical danger, and severe emotional and economic harm. Kraken knew of this danger because it specifically advertised that it implemented security measures to guard against such data breaches and resulting harm.

258. Kraken's negligence was a substantial factor in causing Plaintiff's injuries, and Plaintiff is entitled to recover damages according to proof.

TWELFTH CAUSE OF ACTION

Breach of Confidence

(Against Kraken Defendants)

259. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

260. Plaintiff entrusted Kraken with confidential personal information, including identity documents, address, contact details, and account information, with the reasonable expectation that such information would be kept confidential and used only for legitimate purposes.

261. Kraken breached this duty of confidence by disclosing Plaintiff's confidential

information to criminals through unverified fake legal process and by failing to prevent or promptly remedy the disclosure.

262. As a direct and proximate result, Plaintiff suffered significant harm, including the catastrophic security, emotional, and economic damages described herein, and is entitled to compensatory and punitive damages.

THIRTEENTH CAUSE OF ACTION

Negligent Infliction of Emotional Distress

(Against Kraken Defendants)

263. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

264. Kraken owed Plaintiff a duty to exercise reasonable care in handling his personal information and in safeguarding him, as a known high-value account holder, from foreseeable criminal targeting.

265. Kraken breached this duty through the negligent acts and omissions described above, including the release of unverified data and the delayed breach notification.

266. As a result, Plaintiff has suffered serious emotional distress, including PTSD symptoms, anxiety, sleep disturbances, hypervigilance, and loss of enjoyment of life, which a reasonable person in his position would find intolerable.

267. Kraken's negligence was a substantial factor in causing Plaintiff's severe emotional distress, and Plaintiff is entitled to damages for such distress.

FOURTEENTH CAUSE OF ACTION

Invasion of Privacy – Public Disclosure of Private Facts

(Against All Defendants)

268. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

269. Defendants publicly disclosed private facts about Plaintiff, including his address, date of birth, account username, and the existence and scale of his

cryptocurrency holdings, to persons and entities with no legitimate need or right to such information.

270. These facts are not of legitimate public concern, and their disclosure would be highly offensive to a reasonable person in Plaintiff's position, particularly given the heightened risk of kidnapping and extortion.

271. Defendants acted with malice and willful disregard (or at the very least, negligence, in Kraken's case) for Plaintiff's privacy rights, and as a direct and proximate result, Plaintiff suffered the harms described above and is entitled to damages and injunctive relief.

FIFTEENTH CAUSE OF ACTION

Fraudulent Concealment

(Against Kraken Defendants)

272. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

273. Kraken knew that Plaintiff's personal information had been released to criminals in response to fake legal requests and that Plaintiff, as a high-value account holder, faced extreme physical and economic danger as a result.

274. Kraken had a duty to disclose these material facts to Plaintiff promptly but intentionally concealed them for 39 days, during which time Plaintiff remained unaware of the full extent and source of the threat.

275. Kraken concealed these facts with the intent to deflect responsibility and minimize reputational and legal exposure, and expected Plaintiff to remain ignorant of the true cause of the attacks against him.

276. Plaintiff justifiably relied on Kraken's silence and misleading assurances (such as that Kraken had acted "in good faith") and was thereby prevented from taking earlier and more effective protective measures.

277. As a direct and proximate result of Kraken's fraudulent concealment, Plaintiff suffered the extensive harms described above and is entitled to compensatory and punitive

damages.

SIXTEENTH CAUSE OF ACTION

Misappropriation of Confidential Information

(Against All Defendants)

278. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

279. Plaintiff's personal identifying and account information constituted confidential information of significant economic and security value, which Plaintiff took reasonable measures to protect by providing it only to Kraken under terms promising confidentiality.

280. Kraken misappropriated this confidential information by disclosing it without authorization or legal justification to third-party criminals through forged legal process, and the Roe Defendants misappropriated it by obtaining, using, and further disseminating it for their own benefit.

281. Defendants knew or should have known that they were not authorized to use or disclose Plaintiff's confidential information in this manner.

282. As a direct and proximate result, Plaintiff suffered severe economic, emotional, and security harms and is entitled to damages and equitable relief, including a constructive trust and injunctive orders.

SEVENTEENTH CAUSE OF ACTION

Conversion

(Against Roe Defendants)

283. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

284. Plaintiff has an ownership interest and right to possession in his personal identifying information and account data.

285. The Roe Defendants wrongfully exercised dominion and control over this property by fraudulently obtaining it through fake legal requests and using it for purposes

adverse to Plaintiff's rights, including surveillance, intimidation, and attempted extortion.

286. The Roe Defendants' interference with Plaintiff's property rights was intentional, substantial, and unjustified.

287. As a direct and proximate result, Plaintiff suffered the harms described above and is entitled to damages for conversion according to proof at trial.

EIGHTEENTH CAUSE OF ACTION

Aiding and Abetting Conversion

(Against Kraken Defendants)

288. Plaintiff repeats and incorporates by reference the allegations contained in the preceding paragraphs as though fully set forth herein.

289. The Roe Defendants committed conversion of Plaintiff's personal identifying information and account data as alleged in the Seventeenth Cause of Action.

290. Kraken had actual knowledge, or consciously avoided such knowledge, that the forged requests were being used to obtain and wrongfully control Plaintiff's personal information for unlawful purposes.

291. By disclosing Plaintiff's information without verification, Kraken substantially assisted and enabled the Roe Defendants' conversion.

292. Without Kraken's assistance, the Roe Defendants would not have obtained the detailed personal and account information that formed the basis of their criminal scheme.

293. As a direct and proximate result of Kraken's aiding and abetting conversion, Plaintiff suffered the extensive harms described above and is entitled to damages and equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendants as follows:

Compensatory Damages

1. For general damages according to proof at trial, including damages for:

a. Economic losses (relocation costs, property loss, business harm, security

costs);

b. Non-economic damages (emotional distress, fear, anxiety, loss of enjoyment of life, family separation);

c. Physical harm and stress-related health effects;

d. Ongoing security costs;

2. For special damages according to proof at trial;

3. For statutory damages pursuant to California Civil Code §1708.89 in the amount of not less than $1,500 and not more than $30,000 per violation;

Punitive Damages

4. For punitive damages in an amount sufficient to punish Defendants and deter similar conduct, given the malicious, oppressive, and fraudulent nature of their actions, including pursuant to California Penal Code §§502(e)(4) and 528.5(e);

Attorney's Fees and Costs

5. For reasonable attorney's fees and costs pursuant to:

a. California Civil Code §1708.89(c)(4);

b. California Code of Civil Procedure §1021.5;

c. California Penal Code §502(e)(2) (pursuant to Cal. Pen. C. §528.5(e));

d. Any other applicable statute or legal theory;

6. For pre-judgment and post-judgment interest at the legal rate;

Equitable Relief

7. For a temporary restraining order, preliminary injunction, and permanent injunction:

a. Ordering all Defendants to cease and desist from any further use, disclosure, or dissemination of Plaintiff's personal identifying information;

b. Ordering all Defendants to destroy all copies of Plaintiff's personal identifying information in their possession or control;

c. Ordering Kraken to implement enhanced security measures, including mandatory verification of all law enforcement requests;

d. Ordering Kraken to disclose all information in its possession regarding the identities of the Roe Defendants;

e. Maintaining the confidentiality of Plaintiff's identity and pseudonym;

f. Ordering preservation of all evidence;

8. For restitution and disgorgement of ill-gotten gains;

9. For a constructive trust over any property wrongfully obtained;

10. For an accounting of Defendants' wrongful use of Plaintiff's information;

Relief Under Unfair Competition Law

11. For injunctive relief pursuant to California Business and Professions Code §17203;

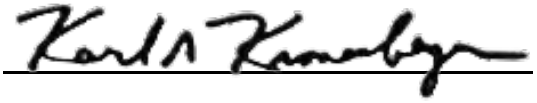
12. For restitution of money and property pursuant to California Business and Professions Code §17203;

13. For such other and further relief as the Court deems just and proper.

Respectfully Submitted,

DATED: March 6, 2026

KRONENBERGER ROSENFELD, LLP

By: 

Karl S. Kronenberger
Leah Rosa Vulić
Galen K. Cheney (*pro hac vice* forthcoming)

Attorneys for Plaintiff JOHN DOE

REQUEST FOR JURY TRIAL

Plaintiff hereby demands a trial of this action by jury of all issues that may be tried to the jury.

Respectfully Submitted,

DATED: March 6, 2026

KRONENBERGER ROSENFELD, LLP

By: _____
Karl S. Kronenberger

Attorneys for Plaintiff JOHN DOE

EXHIBIT A

Terms of Service

Last updated: September 27th, 2016

PLEASE READ THESE TERMS OF SERVICE CAREFULLY. BY CLICKING THE "CREATE ACCOUNT" BUTTON OR BY ACCESSING OR USING THE SERVICES, YOU AGREE TO BE LEGALLY BOUND BY THESE TERMS OF SERVICE AND ALL TERMS INCORPORATED BY REFERENCE.

Summary of Terms of Service

This summary of our Terms of Service offers you an overview of the key terms that apply to your use of our website and trading services. While we hope this summary section is helpful, you should read the **complete Terms of Service** below since they provide important information about how our services work. Please note that we refer to our online service where you can execute trades as "**Kraken**".

Kraken provides you with a platform that matches your trades with open orders from other users of our services at your direction. Users are not able to predetermine a trade with a particular user or with a particular account. Additionally, an order may be partially filled or may be filled by multiple matching orders.

Our Services

Kraken provides you with a simple and convenient way to trade legal tender (such as U.S. dollars and Euros) for digital assets (such as bitcoins and ripples) and vice versa, and to trade one type of digital asset for another type of digital asset. You may also use our Services to purchase and sell digital assets directly from and to us. Our services do not provide users with the ability to trade one form of legal tender for another form of legal tender. Additionally, the range of services available to you will depend in part upon the country or U.S. state from which you access Kraken.

Eligibility and Acceptable Use

You must meet certain **eligibility** criteria to use Kraken. For instance, you must be an adult and there are certain locations from which you may not be able to use some or all of Kraken. Additionally, there are certain things you cannot do when using Kraken, such as engage in illegal activities, lie, or do anything that would cause damage to our services or systems. Please see the **acceptable use section** for more details.

Trading Risks

Engaging in trades may be risky, especially if you engage in any **margin trades** or use any other sophisticated **trading options**. Please don't use Kraken or any of the trading options if you do not understand these **risks**.

Other Important Legal Terms

There are important legal terms provided below in the complete Terms of Service, including your **indemnification responsibilities**, our **limitation of liability** and **warranty disclaimers**, and your agreement to **arbitrate** most disputes. Please take the time to read these terms carefully. You can always contact us through support if you have any questions **https://support.kraken.com**.

1. Complete Terms of Service

These Terms of Service and any terms expressly incorporated herein ("**Terms**") apply to your access to and use of the websites and mobile applications provided by Payward, Inc. and its wholly owned subsidiaries (collectively, "**Payward**", "**Kraken**", "**we**", or "**us**"), and the trading and direct sale services provided by Payward as described in these Terms (collectively, our "**Services**").

Key Definition

Capitalized terms not otherwise defined in these Terms will have the following meaning:

1.1. "External Account" means any Financial Account or Digital Asset Account: (i) from which you may load Funds into your Kraken Account, and (ii) to which you may push

Funds from your Kraken Account.

1.2. "Financial Account" means any financial account of which you are the beneficial owner that is maintained by a third party outside of the Services, including, but not limited to third-party payment service accounts or accounts maintained by third party financial institutions.

1.3. "Funds" means Digital Asset and/or Legal Tender.

1.4. "Legal Tender" means any national currency, such as U.S. dollars, that may be used in connection with a purchase or sale of Digital Assets via the Services, and does not include any Digital Asset.

1.5. "Kraken Account" means a user account accessible via the Services where Funds may be stored by Payward on behalf of a user.

1.6. "Digital Asset" means bitcoins, ripples and other digital assets that may be purchased, sold or traded via the Services.

1.7. "Digital Asset Account" means any Digital Asset address or account owned or operated by you that is maintained outside of the Services, and is not owned, controlled or operated by Payward.

2. Eligibility

Payward may not make the Services available in all markets and jurisdictions, and may restrict or prohibit use of the Services from certain U.S. states or foreign jurisdictions ("Restricted Locations"). If you are registering to use the Services on behalf of a legal entity, you represent and warrant that (i) such legal entity is duly organized and validly existing under the applicable laws of the jurisdiction of its organization; and (ii) you are duly authorized by such legal entity to act on its behalf.

You further represent and warrant that you: (a) are of legal age to form a binding contract (at least 18 years old in the U.S.); (b) have not previously been suspended or removed from using our Services; (c) have full power and authority to enter into this agreement and in doing so will not violate any other agreement to which you are a party; (d) are not located in, under the control of, or a national or resident of (i) any Restricted Locations, or (ii) any country to which the United States has embargoed goods or services; (e) are not identified as a "Specially Designated National;" (f) are not placed on the Commerce Department's

Denied Persons List; and (g) will not use our Services if any applicable laws in your country prohibit you from doing so in accordance with these Terms.

3. Kraken Account

Capitalized terms not otherwise defined in these Terms will have the following meaning:

3.1. Number of Kraken Accounts. Payward may, in its sole discretion, limit the number of Kraken Accounts that you may hold, maintain or acquire.

3.2. Kraken Account information and security. In order to engage in any trades via the Services, you must create a Kraken Account and provide any requested information. When you create a Kraken Account, you agree to: (a) create a strong password that you do not use for any other website or online service; (b) provide accurate and truthful information; (c) maintain and promptly update your Kraken Account information; (d) maintain the security of your Kraken Account by protecting your password and restricting access to your Kraken Account; (e) promptly notify us if you discover or otherwise suspect any security breaches related to your Kraken Account; and (f) take responsibility for all activities that occur under your Kraken Account and accept all risks of any authorized or unauthorized access to your Kraken Account, to the maximum extent permitted by law.

4. Privacy Policy

Please refer to our **Privacy Policy** for information about how we collect, use and share your information.

5. General Obligations

This Section 5 applies to: (i) all trades completed via the Services, (ii) your purchase and/or sale of Digital Assets directly from Payward via the Services, and (iii) any transaction in which you load Funds into your Kraken Account from your External Account or push Funds from your Kraken Account into an External Account.

5.1. **Conditions and Restrictions.** We may, at any time and in our sole discretion, refuse any trade submitted via the Services, impose limits on the trade amount permitted via the Services or impose any other conditions or restrictions upon your use of the Services

without prior notice. For example, we may limit the number of open orders that you may establish via the Services or we may restrict trades from certain locations.

5.2. **Accuracy of Information.** You must provide any information required when creating a Kraken Account or when prompted by any screen displayed within the Services. You represent and warrant that any information you provide via the Services is accurate and complete.

5.3. **Cancellations** You may only cancel an order initiated via the Services if such cancellation occurs before Payward executes the transaction. **Once your order has been executed, you may not change, withdraw or cancel your authorization for Payward to complete such transaction.** If an order has been partially filled, you may cancel the unfilled remainder unless the order relates to a market trade. We reserve the right to refuse any cancellation request associated with a market order once you have submitted such order. **In contrast to exchange orders, all trades are irreversible once initiated.** While we may, at our sole discretion, reverse a trade under certain extraordinary conditions, a customer does not have a right to a reversal of a trade.

5.4. **Insufficient Funds.** If you have an insufficient amount of Funds in your Kraken Account to complete an order via the Services, we may cancel the entire order or may fulfill a partial order using the amount of Funds currently available in your Kraken Account, less any fees owed to Payward in connection with our execution of the trade (as described in Section 9 below).

5.5. **Taxes.** It is your responsibility to determine what, if any, taxes apply to the trades you complete via the Services, and it is your responsibility to report and remit the correct tax to the appropriate tax authority. You agree that Payward is not responsible for determining whether taxes apply to your trades or for collecting, reporting, withholding or remitting any taxes arising from any trades.

6. Kraken Account Funds

6.1. **Funding your Kraken Account.** In order to complete an order or trade via the Services (as described in Section 7), you must first load Funds to your Kraken Account using one of the approved External Accounts identified via the Services. You may be required to verify that you control the External Account that you use to load Funds to your Kraken Account. As further described in Section 9, you may be charged fees by the External Account you use to fund your Kraken Account. Payward is not responsible for any External Account fees or for the management and security of any External Account. You are solely responsible for your

use of any External Account, and you agree to comply with all terms and conditions applicable to any External Account. The timing associated with a load transaction will depend in part upon the performance of third parties responsible for maintaining the applicable External Account, and Payward makes no guarantee regarding the amount of time it may take to load Funds into your Kraken Account.

About Funds Held In Your Kraken Account - Be advised that fiat funds held in your Kraken account are exclusively for the purchase of Digital Assets or withdrawal to your approved External Account. Proceeds from the sale of Digital Assets will be credited to your fiat account, less any transactional or other fees. Furthermore, be advised that Kraken does not pay interest on free fiat balances held in your account.

Digital Assets Only Accounts - If you have opened a Kraken Account designated as Digital Assets Only, you may only fund your account with digital assets. Kraken will not accept fiat to fund a Digital Assets Only Account. If fiat is transmitted to fund such an account, it will be returned to the sender, less applicable transfer fees.

6.2. **Pushing Funds to an External Account.** Provided that the balance of Funds in your Kraken Account is greater than any minimum balance requirements needed to satisfy any of your open positions, you may push any amount of Funds, up to the total amount of Funds in your Kraken Account in excess of such minimum balance requirements, from your Kraken Account to an External Account, less any fees charged by Payward for such transactions (as described in the **Fee Schedule** at the time of your request to push Funds to an External Account).

6.3. **Load/Push Authorization.** When you request that we load Funds into your Kraken Account from your External Account or request that we push Funds to your External Account from your Kraken Account, you authorize Payward to execute such transaction via the Services.

6.4. **Rejected Transactions.** In some cases, the External Account may reject your Funds or may otherwise be unavailable. You agree that you will not hold Payward liable for any damages resulting from such rejected transactions.

7. Exchange Orders and Trades

This Section applies only when you use the Services to trade Digital Assets for Legal Tender or vice versa, or to trade Digital Assets for another form of Digital Assets. Payward does not purchase, sell, or exchange any Digital Assets on its own behalf, except for trades conducted on behalf of German users where Payward fulfills each order on a spot basis as the counterparty to both sides of the transaction.

7.1. **Authorization.** When you submit a new order via the Services, you authorize Payward to execute a transaction in accordance with such order on a spot basis and charge you any applicable fees (as described in Section 10 below).

7.2. **Independent relationship.** You acknowledge and agree that: (a) Payward is not acting as your broker, intermediary, agent, or advisor or in any fiduciary capacity, and (b) no communication or information provided to you by Payward shall be considered or construed as advice.

7.3. **Trade confirmation.** Once the Services execute your trade, a confirmation will be electronically made available via the Services detailing the particulars of the trade. You acknowledge and agree that the failure of the Services to provide such confirmation shall not prejudice or invalidate the terms of such trade.

7.4. **Trade options.** Please refer to the **Trading Guide**, for information about the terminology used in connection with the trading options made available via the Services. If you do not understand the meaning of any trade option, we strongly encourage you not to utilize any of those options.

7.5. **Market rates.** If you select a market trade, Payward will attempt, on a commercially reasonable basis, to execute the trade on or close to the prevailing market exchange rate, as defined via the Services. You acknowledge and agree that the exchange rate information made available via our Services may differ from prevailing exchange rates made available via other sources outside of the Services.

7.6. **Market volatility.** Particularly during periods of high volume, illiquidity, fast movement or volatility in the marketplace for any Digital Assets or Legal Tender, the actual market rate at which a market order or trade is executed may be different from the prevailing rate indicated via the Services at the time of your order or trade. You understand that we are not liable for any such price fluctuations. In the event of a market disruption or Force Majeure event (as defined in Section 24), Payward may do one or more of the following: (a) suspend access to the Services; or (b) prevent you from completing any actions via the Services, including closing any open positions. Following any such event, when trading resumes, you acknowledge that prevailing market rates may differ significantly from the rates available prior to such event.

7.7. **Trade Settlement.** Subject to the terms and conditions in these Terms, we will use commercially reasonable efforts to settle trades on a spot basis within two (2) days of the date upon which users have agreed to execute a trade via the Services.

7.8. Margin Trades.

You agree to maintain in your Kraken Account a sufficient amount of Funds to meet any minimum balance requirements imposed by Payward for users to engage in margin trades. You acknowledge that if you do not have sufficient Funds to meet such minimum balance requirements, that Payward may automatically close some or all of your open positions without notice. Payward may modify such minimum balance requirements from time to time, in its sole discretion. If your margin account balance becomes negative, you agree to pay the amount of Funds owed to Payward within 48 hours. You may not trade on a negative margin account.

You acknowledge and agree that you have read our **Margin Disclosure Statement** and understand the risks involved with margin trades.

8. Risk Disclosure

8.1. **Trading risks.** You acknowledge and agree that you shall access and use the Services at your own risk. The risk of loss in trading Digital Asset pairs and Digital Asset and Legal Tender pairs can be substantial. You should, therefore, carefully consider whether such trading is suitable for you in light of your circumstances and financial resources. You should be aware of the following points:

8.1.1. You may sustain a total loss of the Funds in your Kraken Account, and, in some cases, you may incur losses beyond such Funds. If the market moves against your position, you may be called upon by us to provide a substantial amount of additional margin Funds, on short notice, in order to maintain your position. If you do not provide the required Funds within the time required by us, your position may be liquidated at a loss, and you will be liable for any resulting deficit in your Kraken Account.

8.1.2. Under certain market conditions, you may find it difficult or impossible to liquidate a position. This can occur, for example, when the market reaches a daily price fluctuation limit ("limit move"), if there is insufficient liquidity in the market.

8.1.3. Placing contingent orders, such as "stop-loss" or "stop-limit" orders, will not necessarily limit your losses to the intended amounts, since market conditions may make it impossible to execute such orders.

8.1.4. All Digital Asset positions involve risk, and a "spread" position may not be less risky than an outright "long" or "short" position.

8.1.5. The use of leverage can work against you as well as for you and can lead to large losses as well as gains.

ALL OF THE POINTS NOTED ABOVE APPLY TO ALL DIGITAL ASSET PAIR AND DIGITAL ASSET AND LEGAL TENDER PAIR TRADING. THIS BRIEF STATEMENT CANNOT, OF COURSE, DISCLOSE ALL THE RISKS AND OTHER ASPECTS ASSOCIATED WITH THESE TRADES.

8.2. **Internet transmission risks.** You acknowledge that there are risks associated with utilizing an Internet-based trading system including, but not limited to, the failure of hardware, software, and Internet connections. You acknowledge that Payward shall not be responsible for any communication failures, disruptions, errors, distortions or delays you may experience when trading via the Services, howsoever caused.

9. Digital Asset Terms of Sale

This Section applies only when you use the Services to purchase or sell Digital Assets directly from Payward, a service available in limited jurisdictions only.

9.1. **Prices; Availability.** All prices reflect the exchange rates applicable to the purchase or sale of Digital Assets using the Legal Tender or alternative form of Digital Assets identified in your purchase order. All Digital Asset sales and purchases by Payward are subject to availability, and we reserve the right to discontinue the sale and purchase of Digital Assets without notice.

9.2. **Purchase Quotes.** Prior to completing your purchase or sale of Digital Assets from Payward, we will provide notice of the amount of Digital Assets you intend to purchase or sell and the amount of Funds you will be required to pay to Payward to receive such Digital Assets or Legal Tender. You agree to comply with any terms and conditions provided within such notice to complete your purchase transaction.

9.3. **Errors.** In the event of an error, whether via our Services, in a purchase order confirmation, in processing your purchase, or otherwise, we reserve the right to correct such error and revise your purchase transaction accordingly (including charging the correct price) or to cancel the purchase and refund any amount received. Your sole remedy in the event of an error is to cancel your purchase order and obtain a refund of any amount charged.

9.4. **Payment Method.** Only valid payment methods specified by us may be used to purchase Digital Assets. By placing an order to purchase Digital Assets from Payward, you represent

and warrant that (a) you are authorized to use the designated payment method and (b) you authorize us, or our payment processor, to charge your designated payment method. If the payment method you designate cannot be verified, is invalid or is otherwise not acceptable, your purchase order may be suspended or cancelled automatically. You agree to resolve any problems we encounter in order to proceed with your purchase order.

9.5. **No Returns or Refunds.** All sales and purchases of Digital Assets by Payward via the Services are final. We do not accept any returns or provide refunds for your purchase of Digital Assets from Payward, except as otherwise provided in these Terms.

10. Fees

10.1. **Amount of Fees.** You agree to pay Payward the fees for trades completed via our Services ("**Fees**") as made available via the **Fees and Pair Info** ("**Fee Schedule**"), which we may change from time to time. Changes to the Fee Schedule are effective as of the effective date indicated in the posting of the revised Fee Schedule to the Services, and will apply prospectively to any trades that take place following the effective date of such revised Fee Schedule.

10.2. **Third-Party Fees.** In addition to the Fees, your External Account may impose fees in connection with your use of your designated External Account via the Services. Any fees imposed by your External Account provider will not be reflected on the transaction screens containing information regarding applicable Fees. You are solely responsible for paying any fees imposed by an External Account provider.

10.3. **Payment of Fees.** You authorize us, or our designated payment processor, to charge or deduct your Kraken Account Funds for any applicable Fees owed in connection with trades you complete via the Services.

10.4. **Collection-Related Costs.** If you fail to pay Fees or any other amounts owed to Payward under these Terms and Payward refers your account(s) to a third party for collection, then Payward will charge you the lesser of an 18% collection fee or the maximum percentage permitted by applicable law, to cover Payward's collection-related costs.

11. Electronic Notices

11.1. **Consent to Electronic Delivery.** You agree and consent to receive electronically all communications, agreements, documents, receipts, notices and disclosures (collectively, "**Communications**") that Payward provides in connection with your Kraken Account and/or use of the Payward Services. You agree that Payward may provide these Communications to you by posting them via the Services, by emailing them to you at the email address you provide, and/or by sending an SMS or text message to a mobile phone number that you provide. Your carrier's normal, messaging, data and other rates and fees may apply to any mobile Communications. You should maintain copies of electronic Communications by printing a paper copy or saving an electronic copy. You may also contact us through support **https://support.kraken.com** to request additional electronic copies of Communications or, for a fee, paper copies of Communications (as described below).

11.2. **Hardware and Software Requirements.** In order to access and retain electronic Communications, you will need a computer with an Internet connection that has a current web browser with cookies enabled and 128-bit encryption. You will also need to have a valid email address on file with Payward and have sufficient storage space to save past Communications or an installed printer to print them.

11.3. **Withdrawal of Consent.** You may withdraw your consent to receive electronic Communications by sending a withdrawal notice to support **https://support.kraken.com**. If you decline or withdraw consent to receive electronic Communications, Payward may suspend or terminate your use of the Services.

11.4. **Requesting Paper Copies.** If, after you consent to receive Communications electronically, you would like a paper copy of a Communication we previously sent you, you may request a copy within 30 days after the date we provided the Communication to you by contacting support **https://support.kraken.com**. In order for us to send paper copies to you, you must have a current street address on file with Payward. Please note that Kraken operates exclusively online and it is very burdensome for us to produce paper copies of Communications. Therefore, if you request paper copies, you understand and agree that Payward may charge you a processing fee, in the amount described in the **Fee Schedule**, for each page of Communication requested.

11.5. **Updating Contact Information.** It is your responsibility to keep your email address and/or mobile phone number on file with Payward up to date so that Payward can communicate with you electronically. You understand and agree that if Payward sends you an electronic Communication but you do not receive it because your email address or mobile phone number on file is incorrect, out of date, blocked by your service provider, or you are otherwise unable to receive electronic Communications, Payward will be deemed to have provided the Communication to you. Please note that if you use a spam filter that blocks or

re-routes emails from senders not listed in your email address book, you must add Payward to your email address book so that you will be able to receive the Communications we send to you. You can update your email address, mobile phone number or street address at any time by logging into your Kraken Account or by sending such information to support **https://support.kraken.com**. If your email address or mobile phone number becomes invalid such that electronic Communications sent to you by Payward are returned, Payward may deem your account to be inactive, and you may not be able to complete any transaction via our Services until we receive a valid, working email address or mobile phone number from you.

12. Unclaimed Property

If for any reason Payward is holding Funds in your Kraken Account on your behalf, and Payward is unable to return your Funds to your designated External Account after a period of inactivity, then Payward may report and remit such Funds in accordance with applicable state unclaimed property laws.

13. ACCEPTABLE USE

When accessing or using the Services, you agree that you will not violate any law, contract, intellectual property or other third-party right or commit a tort, and that you are solely responsible for your conduct while using our Services. Without limiting the generality of the foregoing, you agree that you will not:

Use our Services in any manner that could interfere with, disrupt, negatively affect or inhibit other users from fully enjoying our Services, or that could damage, disable, overburden or impair the functioning of our Services in any manner;

Use our Services to pay for, support or otherwise engage in any illegal gambling activities; fraud; money-laundering; or terrorist activities; or other illegal activities;

Use any robot, spider, crawler, scraper or other automated means or interface not provided by us to access our Services or to extract data;

Use or attempt to use another user's account without authorization;

Attempt to circumvent any content filtering techniques we employ, or attempt to access any service or area of our Services that you are not authorized to access;

Develop any third-party applications that interact with our Services without our prior written consent;

Provide false, inaccurate, or misleading information; and

Encourage or induce any third party to engage in any of the activities prohibited under this Section.

14. Feedback

We will own exclusive rights, including all intellectual property rights, to any feedback, suggestions, ideas or other information or materials regarding Payward or our Services that you provide, whether by email, posting through our Services or otherwise ("Feedback"). Any Feedback you submit is non-confidential and shall become the sole property of Payward. We will be entitled to the unrestricted use and dissemination of such Feedback for any purpose, commercial or otherwise, without acknowledgment or compensation to you. You waive any rights you may have to the Feedback (including any copyrights or moral rights). Do not send us Feedback if you expect to be paid or want to continue to own or claim rights in them; your idea might be great, but we may have already had the same or a similar idea and we do not want disputes. We also have the right to disclose your identity to any third party who is claiming that any content posted by you constitutes a violation of their intellectual property rights, or of their right to privacy. We have the right to remove any posting you make on our website if, in our opinion, your post does not comply with the content standards set out in this section.

15. Copyrights and Other Intellectual Property Rights

Unless otherwise indicated by us, all copyright and other intellectual property rights in all content and other materials contained on our website or provided in connection with the Services, including, without limitation, the Payward or Kraken logo and all designs, text, graphics, pictures, information, data, software, sound files, other files and the selection and arrangement thereof (collectively, "**Payward Materials**") are the proprietary property of Payward or our licensors or suppliers and are protected by U.S. and international copyright laws and other intellectual property rights laws.

We hereby grant you a limited, nonexclusive and non-sublicensable license to access and use the Payward Materials for your personal or internal business use. Such license is subject to these Terms and does not permit (a) any resale of the Payward Materials; (b) the distribution, public performance or public display of any Payward Materials; (c) modifying

or otherwise making any derivative uses of the Payward Materials, or any portion thereof; or (d) any use of the Payward Materials other than for their intended purposes. The license granted under this Section will automatically terminate if we suspend or terminate your access to the Services.

16. Trademarks

"Payward," "Kraken," the Kraken logo, the Payward logo and any other Payward product or service names, logos or slogans that may appear on our Services are trademarks of Payward, in the United States and in other countries, and may not be copied, imitated or used, in whole or in part, without our prior written permission. You may not use any trademark, product or service name of Payward without our prior written permission, including without limitation any metatags or other "hidden text" utilizing any trademark, product or service name of Payward. In addition, the look and feel of our Services, including all page headers, custom graphics, button icons and scripts, is the service mark, trademark and/or trade dress of Payward and may not be copied, imitated or used, in whole or in part, without our prior written permission. All other trademarks, registered trademarks, product names and company names or logos mentioned through our Services are the property of their respective owners. Reference to any products, services, processes or other information, by name, trademark, manufacturer, supplier or otherwise does not constitute or imply endorsement, sponsorship or recommendation by us.

17. Third-Party Content

In using our Services, you may view content provided by third parties, including links to web pages of such parties, including but not limited to Facebook and Twitter links ("Third-Party Content"). We do not control, endorse or adopt any Third-Party Content and shall have no responsibility for Third-Party Content, including without limitation material that may be misleading, incomplete, erroneous, offensive, indecent or otherwise objectionable. In addition, your business dealings or correspondence with such third parties are solely between you and the third parties. We are not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings, and you understand that your use of Third-Party Content, and your interactions with third parties, is at your own risk.

18. Suspension; Termination

In the event of any Force Majeure Event (as defined in Section 23.5), breach of this agreement, or any other event that would make provision of the Services commercially unreasonable for Payward, we may, in our discretion and without liability to you, with or without prior notice, suspend your access to all or a portion of our Services. We may terminate your access to the Services in our sole discretion, immediately and without prior notice, and delete or deactivate your Kraken Account and all related information and files in such account without liability to you, including, for instance, in the event that you breach any term of these Terms. In the event of termination, Payward will attempt to return any Funds stored in your Kraken Account not otherwise owed to Payward, unless Payward believes you have committed fraud, negligence or other misconduct.

19. Discontinuance of Services

We may, in our sole discretion and without liability to you, with or without prior notice and at any time, modify or discontinue, temporarily or permanently, any portion of our Services.

20. Disclaimer of Warranties

EXCEPT AS EXPRESSLY PROVIDED TO THE CONTRARY IN A WRITING BY US, OUR SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. WE EXPRESSLY DISCLAIM, AND YOU WAIVE, ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT AS TO OUR SERVICES, INCLUDING THE INFORMATION, CONTENT AND MATERIALS CONTAINED THEREIN.

YOU ACKNOWLEDGE THAT INFORMATION YOU STORE OR TRANSFER THROUGH OUR SERVICES MAY BECOME IRRETRIEVABLY LOST OR CORRUPTED OR TEMPORARILY UNAVAILABLE DUE TO A VARIETY OF CAUSES, INCLUDING SOFTWARE FAILURES, PROTOCOL CHANGES BY THIRD PARTY PROVIDERS, INTERNET OUTAGES, FORCE MAJEURE EVENT OR OTHER DISASTERS INCLUDING THIRD PARTY DDOS ATTACKS, SCHEDULED OR UNSCHEDULED MAINTENANCE, OR OTHER CAUSES EITHER WITHIN OR OUTSIDE OUR CONTROL. YOU ARE SOLELY RESPONSIBLE FOR BACKING UP AND MAINTAINING DUPLICATE COPIES OF ANY INFORMATION YOU STORE OR TRANSFER THROUGH OUR SERVICES.

Some jurisdictions do not allow the disclaimer of implied terms in contracts with consumer, so some or all of the disclaimers in this section may not apply to you.

21. Limitation of Liability

(a) EXCEPT AS OTHERWISE REQUIRED BY LAW, IN NO EVENT SHALL Payward, OUR DIRECTORS, MEMBERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY OTHER DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO LOSS OF USE, LOSS OF PROFITS OR LOSS OF DATA, WHETHER IN AN ACTION IN CONTRACT, TORT (INCLUDING BUT NOT LIMITED TO NEGLIGENCE) OR OTHERWISE, ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF OR INABILITY TO USE OUR SERVICES OR THE Payward MATERIALS, INCLUDING WITHOUT LIMITATION ANY DAMAGES CAUSED BY OR RESULTING FROM RELIANCE BY ANY USER ON ANY INFORMATION OBTAINED FROM Payward, OR THAT RESULT FROM MISTAKES, OMISSIONS, INTERRUPTIONS, DELETION OF FILES OR EMAIL, ERRORS, DEFECTS, VIRUSES, DELAYS IN OPERATION OR TRANSMISSION OR ANY FAILURE OF PERFORMANCE, WHETHER OR NOT RESULTING FROM A FORCE MAJEURE EVENT, COMMUNICATIONS FAILURE, THEFT, DESTRUCTION OR UNAUTHORIZED ACCESS TO Payward'S RECORDS, PROGRAMS OR SERVICES.

Some jurisdictions do not allow the exclusion of certain warranties or the limitation or exclusion of liability for incidental or consequential damages. Accordingly, some of the limitations of this section may not apply to you.

(b) TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF Payward (INCLUDING OUR DIRECTORS, MEMBERS, EMPLOYEES AND AGENTS), WHETHER IN CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE, WHETHER ACTIVE, PASSIVE OR IMPUTED), PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, ARISING OUT OF OR RELATING TO THE USE OF, OR INABILITY TO USE, Payward OR TO THESE TERMS EXCEED THE FEES PAID BY YOU TO Payward DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE DATE OF ANY CLAIM GIVING RISE TO SUCH LIABILITY.

22. Indemnity

You agree to defend, indemnify and hold harmless Payward (and each of our officers, directors, members, employees, agents and affiliates) from any claim, demand, action, damage, loss, cost or expense, including without limitation reasonable attorneys' fees, arising out or relating to (a) your use of, or conduct in connection with, our Services; (b) any Feedback you provide; (c) your violation of these Terms; or (d) your violation of any rights of any other person or entity. If you are obligated to indemnify us, we will have the right, in our

sole discretion, to control any action or proceeding (at our expense) and determine whether we wish to settle it.

23. Applicable Law; Arbitration

PLEASE READ THE FOLLOWING PARAGRAPH CAREFULLY BECAUSE IT REQUIRES YOU TO ARBITRATE DISPUTES WITH US AND IT LIMITS THE MANNER IN WHICH YOU CAN SEEK RELIEF.

You and Payward agree to arbitrate any dispute arising from these Terms or your use of the Services, except for disputes in which either party seeks equitable and other relief for the alleged unlawful use of copyrights, trademarks, trade names, logos, trade secrets or patents. ARBITRATION PREVENTS YOU FROM SUING IN COURT OR FROM HAVING A JURY TRIAL. You and Payward agree to notify each other in writing of any dispute within thirty (30) days of when it arises. Notice to Payward shall be sent to **legal@kraken.com**. You and Payward further agree: (a) to attempt informal resolution prior to any demand for arbitration; (b) that any arbitration will occur in San Francisco, California; (c) that arbitration will be conducted confidentially by a single arbitrator in accordance with the rules of JAMS; and (d) that the state or federal courts in San Francisco, California have exclusive jurisdiction over any appeals of an arbitration award and over any suit between the parties not subject to arbitration. Other than class procedures and remedies discussed below, the arbitrator has the authority to grant any remedy that would otherwise be available in court. Any dispute between the parties will be governed by these Terms and the laws of the State of California and applicable United States law, without giving effect to any conflict of laws principles that may provide for the application of the law of another jurisdiction. Whether the dispute is heard in arbitration or in court, you and Payward will not commence against the other a class action, class arbitration or representative action or proceeding.

24. Miscellaneous

Entire Agreement; Order of Precedence. These Terms contain the entire agreement, and supersede all prior and contemporaneous understandings between the parties regarding the Services. These Terms do not alter the terms or conditions of any other electronic or written agreement you may have with Payward for the Services or for any other Payward product or service or otherwise. In the event of any conflict between these Terms and any other agreement you may have with Payward, the terms of that other agreement will control only if these Terms are specifically identified and declared to be overridden by such other agreement.

Amendment. We reserve the right to make changes or modifications to these Terms from time to time, in our sole discretion. If we make changes to these Terms, we will provide you with notice of such changes, such as by sending an email, providing notice on the homepage of the Site and/or by posting the amended Terms via the applicable Payward websites and mobile applications and updating the "Last Updated" date at the top of these Terms. The amended Terms will be deemed effective immediately upon posting for any new users of the Services. In all other cases, the amended Terms will become effective for preexisting users upon the earlier of either: (i) the date users click or press a button to accept such changes, or (ii) continued use of our Services 30 days after Payward provides notice of such changes. Any amended Terms will apply prospectively to use of the Services after such changes become effective. If you do not agree to any amended Terms, you must discontinue using our Services and contact us to terminate your account.

Waiver. Our failure or delay in exercising any right, power or privilege under these Terms shall not operate as a waiver thereof.

Severability. The invalidity or unenforceability of any of these Terms shall not affect the validity or enforceability of any other of these Terms, all of which shall remain in full force and effect.

Force Majeure Events. Payward shall not be liable for (1) any inaccuracy, error, delay in, or omission of (i) any information, or (ii) the transmission or delivery of information; (2) any loss or damage arising from any event beyond Payward's reasonable control, including but not limited to flood, extraordinary weather conditions, earthquake, or other act of God, fire, war, insurrection, riot, labor dispute, accident, action of government, communications, power failure, or equipment or software malfunction or any other cause beyond Payward's reasonable control (each, a "**Force Majeure Event**").

Assignment. You may not assign or transfer any of your rights or obligations under these Terms without prior written consent from Payward, including by operation of law or in connection with any change of control. Payward may assign or transfer any or all of its rights under these Terms, in whole or in part, without obtaining your consent or approval.

Headings. Headings of sections are for convenience only and shall not be used to limit or construe such sections.

Survival. 23.8 Sections 2 (Eligibility), Section 3 (Kraken Account), 8 (Risk Disclosure), 10 (Fees), 12 (Unclaimed Property), 14 (Feedback), 15 (Copyrights), 16 (Trademarks), 17 (Third-Party Content), 20 (Disclaimer of Warranties), 21 (Limitation of Liability); 22 (Indemnity), 23 (Applicable Law; Arbitration) and this Section 24 (Miscellaneous) shall survive any termination or expiration of these Terms.

Margin Disclosure Statement

We are furnishing this document to you to provide some basic facts about purchasing digital assets or legal tender on margin, and to alert you to the risks involved with trading assets in a margin account. Before trading assets in a margin account, you should carefully review this margin disclosure statement. Please contact us through support **https://support.kraken.com** regarding any questions or concerns you may have with your margin accounts.

When you purchase digital assets for legal tender or vice versa, you may pay in full or you may borrow part of the purchase price from us. If you choose to borrow funds from us, you will open a margin account. The assets purchased are our collateral for the loan to you. If the assets in your account declines in value, so does the value of the collateral supporting your loan, and, as a result, we can take action, such as issue a margin call and/or sell assets in your account, in order to maintain the required equity in the account.

It is important that you fully understand the risks involved in trading assets on margin. These risks include the following:

You can lose more funds than you deposit in the margin account. A decline in the value of assets that are purchased or sold on margin may require you to provide additional funds to us to avoid the forced sale of assets in your account(s).

We can force the sale of assets in your account. If the equity in your account falls below our maintenance margin requirements, we can sell assets in your account to cover the margin deficiency. You also will be responsible for any shortfall in the account after such a sale.

We can sell your assets without contacting you. Customers may mistakenly believe that we must contact them for a margin call to be valid, and that we cannot liquidate assets in their accounts to meet the call unless we have contacted them first. This is not the case. We will attempt to notify you of margin calls, but we are not required to do so. However, even if we have contacted you and provided a specific date by which you can meet a margin call, we can still take necessary steps to protect our financial interests, including immediately selling assets without notice to you.

We can increase maintenance margin requirements at any time and are not required to provide you with advance written notice. These maintenance margin requirements often take effect immediately and may result in the issuance of a maintenance margin call. Your failure to satisfy the call may cause us to liquidate or sell assets in your account(s). We are not responsible to delays in the release of funds intended to satisfy the call, including but not limited to internal holds on funds exceeding verification limits, delays in the transfer of funds from external accounts maintained by third party financial institutions, and failure of proper routing of funds through financial networks. The funds won't count towards their maintenance requirements until the funds are released.

You are not entitled to an extension of time on a margin call. While an extension of time to meet margin requirements may be available to you under certain conditions, a customer

does not have a right to the extension.

Customers with accounts registered in the United States are limited to a 28-day maximum financing term for maintaining open margin positions. Margin positions held beyond 28 days will be automatically liquidated. We are not required to contact you prior to the expiration of the 28-day term and may liquidate your positions without warning. You are expected keep track of your margin positions and settle or otherwise close the positions within 28 days. The 28-day term is fixed and cannot be extended.

Annex A

ADDENDUM: SYNAPSEPAY TERMS

Electronic Fund Transfers ("EFTs") and Account Balances. By creating a Kraken Account and initiating bank deposits or withdrawals (i.e., EFTs), you agree to the terms of service and privacy policy of our financial software provider, SynapsePay, and SynapsePay financial institution partner's Terms of Service & Privacy Policy (**https://synapsepay.com/legal**) ("SynapsePay TOS") which are incorporated herein by reference. Terms not defined in this section shall be defined in SynapsePay TOS.

The Company has partnered with SynapsePay, a financial services software company, to offer you EFTs. When you create a Kraken Account, you may also be prompted to sign up for a SynapsePay User Account (as defined in SynapsePay TOS). You authorize the Company to share your identity and banking information with SynapsePay to open and support your Kraken Account as further detailed in our Privacy Policy and SynapsePay's Privacy Policy (**https://synapsepay.com/legal**). It is your responsibility to make sure the data you provide us is accurate and complete. Additionally, you are responsible for complying with SynapsePay TOS when using your User Account. IT IS YOUR RESPONSIBILITY TO READ AND UNDERSTAND THE SYNAPSEPAY TOS, AS IT CONTAINS TERMS AND CONDITIONS RELATING TO YOUR SYNAPSEPAY USER ACCOUNT, INCLUDING BUT NOT LIMITED TO YOUR RIGHTS, LIMITATIONS, REVERSAL AND OTHER LIABILITIES, LIMITATION OF LIABILITY AND BINDING ARBITRATION PROVISIONS.

Annex B

ADDENDUM: Crypto Facilities Ltd

The Company has partnered with Crypto Facilities Ltd (**https://www.cryptofacilities.com/**) for derivative exchange services. We may use and share your information with Crypto Facilities Ltd and other Payward Entities. This information is used by them and us to assess and process

applications, provide you with products and services and manage their (or our) relationship with you and/or as part of a sale, reorganization, transfer or other transaction relating to our business; and, understand our clients preferences, expectations and financial history in order to improve the products and services we offer.

You authorize the Company to share your identity and banking information with Crypto Facilities to open and support a membership with Crypto Facilities, as further detailed in our Privacy Policy and Crypto Facilities' Privacy Policy (**https://www.cryptofacilities.com/privacy-policy**). It is your responsibility to make sure the data you provide us is accurate and complete. Additionally, you are responsible for complying with Crypto Facilities Membership Agreement (**https://www.cryptofacilities.com/membership-agreement**) when using their services. IT IS YOUR RESPONSIBILITY TO READ AND UNDERSTAND THE CRYPTO FACILITIES MEMBERSHIP AGREEMENT.

Features

24/7 Support
Account Management
API
Bug Bounty
Fee Schedule
Funding Options
Futures
Indices
Liquidity
Margin Trading
OTC
PGP Key
Proof of Reserves
Security
Support
WebSockets

Prices

Cryptowatch
Prices Overview

Learn

Blog
Institutions
Podcast

About

Why Kraken
Careers
Contact
Press

Privacy Notice
Terms of Service
Cookies Policy
U.S. English