

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

August 30, 2022

Mr. Jesse Powell  
Chief Executive Officer and President  
Payward Ventures, Inc.  
d/b/a Kraken  
237 Kearny Street, #102  
San Francisco, CA 94108

Dear Mr. Powell:

I write to request information and documents about the work that Payward Ventures, Inc., d/b/a Kraken (Kraken), is doing to combat cryptocurrency-related fraud. Cryptocurrencies have become scammers' favored means of payment as well as their preferred bait for unsuspecting victims. The annual amount of cryptocurrency lost to fraud is on track to surpass \$1 billion in 2022.<sup>1</sup> Multimillion-dollar cryptocurrency scams have become a regular occurrence.<sup>2</sup> As shown by recent Department of Justice indictments, these scams take many forms, including as commodity scams, fraudulent coin offerings, and sham investment platforms.<sup>3</sup> Given the growing popularity of cryptocurrencies both as a form of payment and as an investment, I am concerned by the rapid growth of fraud and consumer abuse. I am also concerned by the apparent lack of action by cryptocurrency exchanges to protect consumers conducting transactions through their platforms.

Cryptocurrency is a form of digital currency based on an immutable digital ledger technology called blockchain. Cryptocurrency is kept in an anonymous digital wallet and can be bought, sold, or traded. These transactions occur on cryptocurrency exchanges and cannot be reversed once made. Bitcoin, one of the most popular cryptocurrencies, launched in 2009, and

---

<sup>1</sup> Federal Trade Commission, *Data Spotlight: Reports Show Scammers Cashing in on Crypto Craze* (June 3, 2022) (online at [www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze)).

<sup>2</sup> See, e.g., Commodity Futures Trading Commission, *Press Release: CFTC Charges South African Pool Operator and CEO with \$1.7 Billion Fraud Involving Bitcoin* (June 30, 2022) (online at [www.cftc.gov/PressRoom/PressReleases/8549-22](http://www.cftc.gov/PressRoom/PressReleases/8549-22)). See also Department of Justice, *Press Release: BitConnect Founder Indicted in Global \$2.4 Billion Cryptocurrency Scheme* (Feb. 25, 2022) (online at [www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme](http://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme)).

<sup>3</sup> See, e.g., Department of Justice, *Press Release: Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over \$100 Million in Intended Losses* (June 30, 2022) (online at [www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud](http://www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud)).

there are now thousands of cryptocurrencies available. To take advantage of public interest in cryptocurrency, developers use initial coin offerings (ICOs) to secure investments in new cryptocurrencies prior to launch. Despite recent heavy losses to the value of many digital assets, cryptocurrencies continue to have a global market cap in excess of \$1 trillion.

As stories of skyrocketing prices and overnight riches have attracted both professional and amateur investors to cryptocurrencies, scammers have cashed in. The lack of a central authority to flag suspicious transactions in many situations, the irreversibility of transactions, and the limited understanding many consumers and investors have of the underlying technology make cryptocurrency a preferred transaction method for scammers.<sup>4</sup> Consumer interest has also driven the creation of fraudulent cryptocurrencies, in which developers create tokens, list them on exchanges, and generate investments before absconding with investors' dollars. Chainalysis, a blockchain data platform, noted that these so-called "rug pulls" accounted for roughly 37% of cryptocurrency scam revenue 2021, compared to 1% in 2020.<sup>5</sup>

The private sector has taken some steps to protect consumers and investors and curb cryptocurrency fraud. Code audits, where a third-party evaluates the terms of a digital asset, can identify and warn consumers of the vulnerabilities that make fraud schemes possible.<sup>6</sup> Open-source investigators and organizations such as RugDocs conduct audits and warn potential investors of the risks of certain digital assets.<sup>7</sup> Some exchanges also maintain insurance policies to cover consumer losses from criminal activity.<sup>8</sup> However, significant risk remains. Consumers are often unaware of the current patchwork of resources available to inform their investing decisions, and insurance companies are wary to provide insurance to individual consumers given the lack of regulation of digital assets.

---

<sup>4</sup> Federal Trade Commission, *Data Spotlight: Reports Show Scammers Cashing in on Crypto Craze* (June 3, 2022) (online at [www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze](http://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze)). Although FinCEN has released guidance discussing how the Bank Secrecy Act applies to virtual currencies, questions remain as to how well this law can regulate decentralized exchanges that use an automated program to facilitate transactions among a network of users. FinCEN's 2019 guidance notes that a "trading platform [that] only provides a forum where buyers and sellers ... post their bids and offers..., and [where] the parties themselves settle any matched transactions through an outside venue, ... does not qualify as a money transmitter under FinCEN regulations." Department of the Treasury, Financial Crimes Enforcement Network, *Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (FIN-2019-G001) (May 9, 2019) (online at [www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf](http://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf)). Such decentralized exchanges pose significantly greater risks to investors, making regulation particularly important. See, e.g., *6 Common Crypto Scams, and How Investors Can Protect Their Coins*, Next Advisor (May 16, 2022) (online at <https://time.com/nextadvisor/investing/cryptocurrency/common-crypto-scams/>).

<sup>5</sup> Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022) (online at <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>).

<sup>6</sup> *Id.*

<sup>7</sup> *The "Rug Doctor" Who Advises Crypto Investors Against "Horrible" DeFi Scams*, Yahoo Finance (Mar. 5, 2022) (online at <https://finance.yahoo.com/news/this-rug-doctor-has-a-message-for-crypto-investors-hungry-for-de-fi-returns-162804016.html>); *Twitter Vigilantes Are Hunting Down Crypto Scammers*, Wired (Nov. 15, 2021) (online at [www.wired.com/story/twitters-crypto-vigilantes-are-just-getting-started/](http://www.wired.com/story/twitters-crypto-vigilantes-are-just-getting-started/)).

<sup>8</sup> *Can You Insure Bitcoin? Here's What You Need to Know*, CNET (Feb. 23, 2022) (online at [www.cnet.com/personal-finance/crypto/can-you-insure-bitcoin/](http://www.cnet.com/personal-finance/crypto/can-you-insure-bitcoin/)).

While some exchanges review cryptocurrencies before listing them, others allow digital assets to be listed with little or no vetting. Potential vulnerabilities that could easily be identified through code audits are left undiscovered. Insufficient security measures likewise leave users exposed to the outright theft of assets stored on the exchange. Many exchanges have also failed to implement appropriate monitoring of accounts, which can flag illicit activity, notify investors, and prevent transactions with addresses linked to scammers.<sup>9</sup>

For all these reasons, I am concerned about the growth of fraud and consumer abuse linked to cryptocurrencies. Notwithstanding federal regulations, cryptocurrency exchanges must themselves act to protect consumers conducting transactions through their platforms. By implementing audit policies, requiring certain disclosures, delisting, and adopting other safety mechanisms, cryptocurrency exchanges can—and should—create safer environments for consumers.

To assist the Subcommittee in its review of this matter, by September 12, 2022, please produce the following documents dated from the later of January 1, 2009, or the date Kraken was founded to the present:

1. All documents regarding Kraken's efforts to combat crypto-related scams and fraud and inform consumers about the risks related to investments in cryptocurrencies;
2. All documents regarding Kraken's processes to identify, investigate, and remove or flag potentially fraudulent digital assets or accounts used on Kraken's product(s);
3. All documents setting out Kraken's policies governing cryptocurrencies, cryptocurrency traders, buyers, sellers, investors, consumers, or any other individual or entity using Kraken's product(s); and
4. All documents discussing whether to adopt more stringent policies governing cryptocurrencies, cryptocurrency traders, buyers, sellers, investors, consumers, or any other individual or entity using Kraken's product(s).

The Subcommittee also requests answers to the following questions by September 12, 2022:

1. What tools, including but not limited to code audits, security protocols, or incident reporting systems, does Kraken currently have in place to mitigate the risk of fraud or other criminal activity?

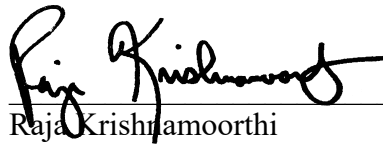
---

<sup>9</sup> Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022) (online at <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>).

2. What mechanisms does Kraken have in place to ensure that individuals selling, purchasing, or investing in digital assets are made aware of the relevant risks?
3. What mechanisms, such as insurance covering fraud or other criminal acts, does Kraken have in place to ensure that individuals harmed while using your services are recompensed?
4. For the topics in questions 1 through 3, what mechanisms does Kraken currently have concrete plans to implement? By when does Kraken intend to have these mechanisms in place?
5. What actions do you believe the federal government could take to assist cryptocurrency exchanges in combatting fraud and scams?

The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. An attachment to this letter provides additional instructions for responding to the Subcommittee’s request. If you have any questions regarding this request, please contact Subcommittee staff at (202) 225-5051.

Sincerely,



Raja Krishnamoorthi  
Chairman

Subcommittee on Economic and Consumer Policy

Enclosure

cc: The Honorable Michael Cloud, Ranking Member  
Subcommittee on Economic and Consumer Policy

## Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
  - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
  - b. Document numbers in the load file should match document Bates numbers and TIF file names.
  - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
  - d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:  
  
BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,  
BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

### **Definitions**

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.