



UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
STATION PLACE  
100 F STREET, NE  
WASHINGTON, DC 20549-2465

Office of FOIA Services

February 19, 2025

Ms. Eva Laverty-Wilson  
History Associates, Inc.  
7361 Calhoun Pl., Suite 310  
Rockville, MD 20855

RE: Freedom of Information Act (FOIA), 5 U.S.C. § 552  
Request No. **24-03754-FOIA**

Dear Ms. Laverty-Wilson:

This letter is in response to your request, dated August 9, 2024, and received in this office on August 12, 2024, for access to "copies of all records, including all investigative files and any other factual documents received by the Commission, any Commissioner, and/or any Commission Staff or otherwise in the Commission Staff's custody or control, or any internal or external communications reflecting or concerning any investigations by the Commission or Commission Staff, of Paxos Trust Company, LLC."

The enclosed 21 pages are released with the exception of third-party names, addresses, telephone numbers, emails, and contract numbers. This information is withheld under 5 U.S.C. § 552(b)(6), because the release of these records would constitute a clearly unwarranted invasion of personal privacy. Please be advised that we have considered the foreseeable harm standard in preparing this response.

Additionally, we are withholding records that may be responsive to your request under 5 U.S.C. § 552(b)(7)(A). This exemption protects from disclosure records compiled for law enforcement purposes, the release of which could reasonably be expected to interfere with enforcement activities. Since Exemption 7(A) protects the records from disclosure, we have not determined if other exemptions apply. Therefore, we reserve the right to assert other exemptions when Exemption 7(A) no longer applies. Please be advised that we have considered the foreseeable harm standard in preparing this response.

It is the general policy of the Commission to conduct its investigations on a non-public basis. Thus, subject to the provisions of FOIA, the Commission does not disclose the existence or non-existence of an investigation or information gathered unless made a matter of public record in proceedings brought before the Commission or in the courts. Accordingly, the assertion of this exemption should not be construed as an indication by the Commission or its staff that any violations of law have occurred with respect to any person, entity, or security. Please be advised that we have considered the foreseeable harm standard in preparing this response.

I am the deciding official with regard to this adverse determination. You have the right to appeal my decision to the SEC's General Counsel under 5 U.S.C. § 552(a)(6), 17 CFR § 200.80(f)(1). The appeal must be received within ninety (90) calendar days of the date of this adverse decision. Your appeal must be in writing, clearly marked "Freedom of Information Act Appeal," and should identify the requested records. The appeal may include facts and authorities you consider appropriate.

You may file your appeal by completing the online Appeal form located at [https://www.sec.gov/forms/request\\_appeal](https://www.sec.gov/forms/request_appeal), or mail your appeal to the Office of FOIA Services of the Securities and Exchange Commission located at Station Place, 100 F Street NE, Mail Stop 2465, Washington, D.C. 20549, or deliver it to Room 1120 at that address.

If you have any questions, please contact Sonja Osborne at [osbornes@sec.gov](mailto:osbornes@sec.gov) or (202) 551-8371. You may also contact me at [foiapa@sec.gov](mailto:foiapa@sec.gov) or (202) 551-7900. You may also contact the SEC's FOIA Public Service Center at [foiapa@sec.gov](mailto:foiapa@sec.gov) or (202) 551-7900. For more information about the FOIA Public Service Center and other options available to you please see the attached addendum.

Sincerely,



Carmen L. Mallon  
FOIA Branch Chief

Enclosures

**ADDENDUM**

For further assistance you can contact a SEC FOIA Public Liaison by calling (202) 551-7900 or visiting <https://www.sec.gov/oso/help/foia-contact.html>.

SEC FOIA Public Liaisons are supervisory staff within the Office of FOIA Services. They can assist FOIA requesters with general questions or concerns about the SEC's FOIA process or about the processing of their specific request.

In addition, you may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA dispute resolution services it offers. OGIS can be reached at 1-877-684-6448 or via e-mail at [ogis@nara.gov](mailto:ogis@nara.gov). Information concerning services offered by OGIS can be found at their website at [Archives.gov](https://www.archives.gov). Note that contacting the FOIA Public Liaison or OGIS does not stop the 90-day appeal clock and is not a substitute for filing an administrative appeal.

**File**

(b)(6)

**Incoming Complaint – Phone Call:**

Correspondent reports that he has an account with crypto.com and a Paxos wallet. He believes he has made money and wants to know about wiring a \$75K security deposit to the firm. He states that they are supposed to return the funds within 24 hours. He plans to get a small loan from the bank to make the transfer and want to confirm that the matter does not involve a scam.

**File** (b)(6)

**Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 2/16/2023

Origin: Web

File #: (b)(6) ~::HO

Send to Entity: Yes

**Investor Information**

Name: (b)(6)

Address: (b)(6)

(b)(6)

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6)@gmail.com

**Entity Information**

Name: Paxos Trust Company

Type: On-Line Trading Firm

Representative: Paxos Team

Address: 450 Lexington Ave Suite 3952

New York, 10017

**Security Information**

Name:

Symbol:

Type: Currency transactions

**Description:**

I hope this letter has correctly found itself within your complaints/fraud department as it is very essential to me that you become aware of the ordeal I have had to go through. Commencing on or around November 26, 2021, I fell victim to a multilayered scam operation orchestrated by Jiansheng Limited.

Money was transferred from my account totaling (b)(6) USDP from my wallet utilizing your services.

**OVERVIEW**

- This letter shall thrust into the spotlight, inter alia, the increasingly important role those financial institutions play in the fight against financial crime and fraud, and the pressing need for enhanced supervision and vigilance within your organization.
- Here's an indisputable fact: had you looked at the wider circumstances surrounding the above- referenced transaction(s), this illicit transfer of wealth could have been prevented.

- Obviously, there is no consensus with respect to the degree and scope to which regulated and licensed financial institutions must intervene and block suspicious transactions, and indeed, in so doing, financial institutions may often cause payments to be slowed down unnecessarily or even some legitimate payments may be rejected, however, please be noted that additional frictions such as slower payments (such as delaying payments or freezing funds to investigate)

is beneficial to and welcomed by vulnerable customers and is widely considered to be a positive practice that is necessary in order to maintain market integrity as well as customers' financial safety, particularly for large-value and/or out-of-pattern payments.

- As demonstrated herein, you are undeniably an involved player in the scam's ecosystem, by providing the infrastructure which fraudsters exploit to make their scams more operable. Responsible financial institutions should work hard and be committed to both the future of the market and the security of all customer funds. You must recognize that you play a critical role over the funds you hold as digital assets for your customers. Acting as a custodian requires a high bar including, but not limited to, appropriate security safeguards that are independently audited and tested on a regular basis.
- As set forth herein, your organization, by its conduct, evidently failed to perform adequate "Anti-Money Laundering" and "Know Your Client" (combined as "AML/KYC") procedures, as those procedures are commonly known under the applicable guidelines and enforcement rules. Combined with appropriate safeguards, AML/KYC could have the potential to prevent the victimization described herein.
- Upon information and belief, the fraudsters liquidated cryptocurrencies through your services for FIAT money; however, the liquidated cryptocurrencies were not legitimately generated revenues. Instead, those cryptocurrencies were stolen through a sophisticated fraudulent scheme. Unbeknownst to myself and to the public, the fraudsters were misappropriating cryptocurrencies from innocent people while liquidating those cryptocurrencies through your services.
- Against this background, and without derogating any of my rights, I hereby hold you liable for financial and emotional harm as well as medical problems relating to this victimization, and demand that you reimburse my account in full within 7 days from the date of this letter.

#### INTRODUCTION

Financial crimes and fraud investigations often involve a high degree of sophistication, complexity, and sensitiveness to detail. Accordingly, this letter aims to address the issue at hand as profoundly and fairly as possible, by taking into consideration contextual regulations, laws, and bylaws, as well as guidance, standards and rules promoted by supervisory authorities, relevant codes of practice, and (where suitable) what was good industry practice (GIP) at all times relevant hereto. The allegations contained herein are predicated either upon knowledge with respect to myself and my own experience, or upon facts obtained through investigations conducted by qualified third parties. I strongly believe that substantive evidence in support of the allegations set forth herein will be found after an appropriate opportunity for discovery. Key facts supporting the allegations contained herein are known only to the Company and/or are exclusively within their control.

The Company cleverly orchestrated a prevalent scheme of deception to lead people to invest significant sums while knowing that those would-be investors would ultimately lose the money, they had entrusted to it. The overall purpose of the scheme, in other words, was to target and defraud people who are often inexperienced and naive, in pursuance of illicit wealth through various fraudulent representations. I did not know, and through the exercise of reasonable diligence could not have discovered, the fraud that was being perpetrated upon me by the Company.

Fraud is commonly conceptualized as withholding from the weaker party in a financial transaction (e.g. an investor) information which is necessary to make an informed, rational or autonomous decision. In this regard, even access to adequate information is insufficient to achieve complete autonomy. A complication here is that the weaker party, amateur/unseasoned investors in particular, might have trouble analyzing the data at hand

sufficiently well to identify fraudulent schemes. Unfortunately, because financial products are often abstract and complex, there is no easy solution to this problem. Therefore, full autonomy of investors might not only require access to sufficient information, but also access to relevant technologies, know-how, processing capabilities, and resources to analyze the information. A reasonable solution is that financial institutions would be required to promote transparent communication in which they understand the business of its customers and its legality.

According to the Federal Trade Commission's interpretations of certain terms (like the words deceptive and unfair), the FTC has found that a "deceptive act or practice" encompasses "a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."

The federal courts have defined a "deceptive trade practice" [ i ] as any act or practice that has the tendency or capacity to deceive consumers and have defined an "unfair trade practice" as any act or practice that offends public policy and is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. The false representations and omissions made by the Company have a tendency or capacity to deceive consumers, such as myself, into unwittingly providing funds that fueled the Company's fraudulent scheme and are therefore by their very nature jointly immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

As a result of the Company's deceptive trade practices, I was deceived into transferring my funds for investment returns that were never delivered. I will certainly never receive any monetary value for the investments considering the way the Company had their scheme rigged thus causing significant economic damage to me. The false statements of material facts and omissions as described above; and the fraudulent transaction(s) the Company perpetrated upon me; were unfair, unconscionable, and deceptive practices perpetrated on me which would have likely deceived any reasonable person under the circumstances.

When determining what is reasonable and fair, we should focus on the issue of liability; Common queries include, but are not limited to, the following: (i) whether you violated any rule, law, or regulation, and/or breached any material elements of the relevant bylaws or codes of conduct, in failing to protect the public's financial safety; (ii) whether by virtue of your custodianship over the funds or by your control over them, you owed a fiduciary duty to the public and if so, whether that duty was breached; (iii) whether you promoted the transaction(s) in question despite being aware of the nature of business in question (iv) whether you were in compliance with your own policies and procedures; (v) whether you owed duties to the public, what the scope of those duties was, and whether you breached those duties; (vi) whether your conduct was unfair or unlawful; (vii) whether you have been unjustly enriched; (viii) whether I have sustained damages as a result of your conduct; and (ix) whether you have within your power the ability to, and should, compensate me for the harm that has befallen me.

#### MERCHANT'S FRAUD SCHEME — ALLEGATIONS

The Company hired, managed, and trained personnel, and collaborated with others as accomplices to their crimes to induce fraud that resulted in my financial and psychological damages. These include, but are not limited to the following allegations all of which involve criminal, non-regulated, and malicious activities:

1. 2.

3.

The Company directed and instructed others to work from shell companies that were operating from various unassociated locations across the globe.

The Company opened bank accounts and established Crypto Wallets in multiple countries and different crypto exchange platforms (including yours) and used them through their accomplices and strawmen from around the world to conceal and disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.

The Company intentionally committed fraudulent misrepresentation, and falsified its agent names, credentials, competencies, qualifications and location. The Company's name is merely a brand name, officially

owned by shell corporations located offshore. In reality, the entire operation is being conducted from elsewhere (supposed location is evidently fictitious), and on top of that the call center, marketing, and decision making, are all being performed by completely anonymous and hidden entities. Concealing true identities and utilizing front companies as a vehicle for a wide spectrum of financial maneuvers is a notorious practice of criminal organizations.

The Company has blatantly violated international laws, as it has been practicing without a license and funneling enormous sums of money, through countries and jurisdictions that require registration to operate.

4.

5. 6.

7. 8. 9. 10. 11. 12.

13. 14. 15. 16.

The Company provided direct investment advice - not utilizing 3rd party recommendations (e.g., "according to Bloomberg TV/Investing.com")

The Company offered investment services/advice not related to real market/exchange data (manufacturing false charts etc.). The trading platform was purposely manipulated in a way that each client would ineluctably and unknowingly lose money, as the trades were simply concocted. Instead, the Company's staff and its accomplices simply pocketed the money, using it to purchase various luxurious, non-essential items, including exotic cars, gadgets, jewelry, drinks, accessories, cosmetics, fragrances, and watches.

The Company prohibited my ability to withdraw my funds.

The Company was guaranteeing returns/yields (unrealistic ones).

The Company furnished me with bonuses - which are not allowed to be given. The Company traded on my behalf (use of remote control of my computer).

My money was not held in a segregated account.

The Company did not advertise/disclose/was not transparent regarding the statistical data representing the percentage of total client losses at the company.

The Company did not mention the commission and overnight swaps.

The Company did not read the risk disclosure prior to my deposit(s).

The Company used high pressure tactics and outbursts, which took a severe toll on my health. Armed with my personal details, the Company's staff seduced me into transferring all of my savings to them. They utilized their knowledge of my cultural context, which stressed square and honorable business dealings along with honesty, in order to maliciously take advantage of my trusting nature.

#### EXPOSING YOUR ORGANIZATION'S MISCONDUCT

Having

organization has completely failed to adequately investigate the fraudster's accounts and has willfully blinded itself to obvious red flags.

Many suspicions should have been arisen at your organization as an issue of great concern, with respect to the unusual activity taking place in my account. Despite the regulatory and statutory requirements your organization should abide by as a licensed and regulated financial institution, and instead of detecting patterns, drawing certain conclusions, and taking actions accordingly, you at best merely and insufficiently performed a minimal hasty and haphazard review of the account(s) held by the fraudsters or possibly asked only a few trivial questions regarding the suspicious activities, and at worst, shut your eyes completely rather than being careful, methodical, and vigilant. Had you analyzed the circumstances surrounding the transactions in question, I hereby allege that your

bothered, you would probably have realized that the funds were associated with fraud and financial crime, rather than some other legitimate revenue/activity.



In light of the above, and after conducting a comprehensive review, it has become glaringly obvious to me that no adequate information and/or documentation were sought by your organization, at best, and at worst —no appropriate safeguards were implemented.

If a financial institution executed a customer's order to transfer money knowing it to be "dishonestly given, shutting its eyes to the obvious fact of the dishonesty or acting recklessly in failing to make such inquiries as an honest and reasonable individual would make," it would be in breach of its AML/CTF/KYC, even if on the surface the payment was in a legal manner (which it clearly was not) the financial institution should still be liable for negligence resulting in damages.

Compliance departments should ensure that staff members understand the legal requirements and where there are suspicions that these suspicions be communicated to all relevant personnel whilst being investigated.

For the avoidance of doubt, reasonable grounds should not necessarily be interpreted as proof. On the basis of various signs, you should have assumed that something fishy was going on and should have suspended transaction(s) until reasonable enquiries could be made to verify that the transaction(s) was/were properly executed. In other words, I am a victim of your negligence for facilitating the misappropriation of funds, and doing little to safeguard public financial interests. Any reasonable staff member would have realized that there were many obvious, even glaring, signs that I was a fraud victim.

Had you cursorily audited or reviewed the Blockchain history of the cryptocurrencies in question, it would have been transparent and beyond obvious to you that those transaction were not in any way legitimate, but were fraudulent in nature.

You knew or should have known that the funds being transferred through your services did not rightfully belong to the recipient fraudsters. Similarly, you knew or should have known that the assets being transferred through your services have no legitimate or lawful purpose.

You turned a blind eye to the crimes that you have facilitated and thus provided an array of essential Crypto transfer services, acting as a vehicle, with the awareness that it was enabling the fraudsters to commit crimes and enrich themselves with victims' assets.

Your services undoubtedly served as a crucial element in the fraudulent scheme detailed herein, and you were either unaware of your complicity in the fraud, or, more worryingly, completely aware yet silent. Had you conducted an adequate account analysis, including proper KYC procedures, you would have discovered my vulnerability, my financial illiteracy, and the nature of my relationship with the recipient. This could have been beneficial for me, as you would have subsequently disclosed and reported the fraudsters' activities to law enforcement authorities in a timely manner. Instead, to satisfy your financial interests, you conveniently closed your eyes, even though you undeniably had, at all material times, the necessary controls and resources to influence, whether directly or indirectly, those particular transactions.

You also had the duty to stop those crimes, yet you refused to do so because you were more interested in enriching yourself, even if it meant furthering those crimes and allowing them to cause massive financial losses to plenty of victims — many of whom are probably your customers. Therefore, it is clear that you did not have in place adequate security measures to properly safeguard my assets — hence, you have irreparably harmed me and, if not enjoined, will continue to irreparably harm other victims as well as their loved ones and associated. You have irreparably harmed the general public and, if not enjoined, will continue to irreparably harm the general public which our society deserves better.

"A financial institution which wrongly pays money away when it has no authority to do so will usually be treated as if it had paid using its own funds, not those of its customer." The debits made to my account should be reversed out, and damages to compensate me for any reasonably foreseeable losses incurred as a result of your failure to state the balance of my account accurately and properly. It is also libelous/defamatory to make false statements about someone that adversely affects their financial status.

When discussing the responsibilities that a financial institution might incur, it is crucial not to forget the fact that a legitimate complaint by, or cause of action on the part of, a client might generate/give rise to further

statutory cause of action or/and additional responsibilities or liabilities beholden by a financial institution to the relevant regulatory authority. Obligations/duties beholden by a financial institution to a regulator are distinct from those beholden to the individual. Moreover, you may be liable to more than one regulator. As a regulated and licensed financial institution, you have strict statutory and regulatory obligations to monitor transactions and report any suspicious activities to law enforcement authorities. The importance of implementing robust internal systems to detect and report money laundering and other suspicious activities has been continuously emphasized in the industry in addition to having the appropriate policies, procedures and internal controls in place to ensure ongoing compliance in respect

of the aforementioned systems. You should have analysed your client's activities and distinguished thereafter between that which may be normal activity as opposed to that which might suggest illegal activity. This is a well-known industry standard which plays a substantial role in preventing criminals from liquidating and laundering customer funds.

#### FRAUD

Actual fraud can be described, *inter alia*, as "suppression of that which is true, by one having knowledge or belief of the fact". Therefore, due to your actual knowledge that such scams are prevalent, you are liable for damages. Similarly, due to the fact that you knew or were grossly negligent in not knowing that those scams should not be entrusted with your customer assets—you are likewise liable for committing actual fraud and thus, are responsible for any damages caused to me as a result.

#### NEGLIGENT MISREPRESENTATION

Your organization, by acts of both omission and commission, whether directly or indirectly, are responsible for false/inaccurate/misleading statements of material facts concerning the services I received. Specifically, your representations to myself, *inter alia*, : (a) you had in place adequate security measures to properly safeguard customer's assets; (b) your organization's technology was, for all intents and purposes, free of any inherent flaws that might expose your customers to transactional irregularities; (c) your organization was able to take full responsibility if things go wrong; and (d) your organization's technology was, for all intents and purposes, free of any inherent flaws that might expose your customers to fraud.

Additionally, it is hereby alleged that your manoeuvres, whether premeditated or not, despite the fact that you expressly establish to promote fairness and customer confidence, are actually used to blind your customers, thereby depriving them of disclosures regarding the involved risk factors, potential threats, and other information required by law.

#### UNJUST ENRICHMENT

By engaging in the conduct described herein, you, directly or indirectly, knowingly and/or with severe recklessness, in particular by not doing enough to fight against financial crime, have reaped the benefits from allowing the transfer of money to the Company, thereby causing actual harm to a substantial amount of people. Retaining the said monetary benefits, as a result of your misconduct alleged herein, is unconscionable and against the fundamental principles of justice.

#### VIOLATIONS OF INTERNATIONAL LAW

By reason of this misconduct, you violated, and if not enjoined will continue to violate, many of the international anti-fraud policies, which are established to facilitate the development of controls that aid in the detection and prevention of worldwide fraud.

Your organization's blatant disregard of its obligation to maintain my financial safety has caused significant, irreparable damage and injury to me. Much of which is clearly a result of negligence or so easily subject to investigation that it is apparent that you misappropriated the funds either knowingly or with reckless disregard to whether these transactions were lawful or not. You have an independent and non-delegable duty to conduct a reasonable investigation of any and all transactions and the failure to do so is a violation of the law and of the rights of those affected by such negligence.

#### AIDING AND ABETTING

By engaging in the conduct described herein, you, knowingly or recklessly, promoted transactions, practices, and courses of business which operate or would operate as a fraud and deceit upon the purchasers and provided substantial assistance to the commission of financial crime. By engaging in the conduct described herein, which no doubt is a substantial factor in causing my injuries, you aided and abetted the Company and if not enjoined, will continue to aid and abet violations.

As a direct, foreseeable, and proximate result of your conduct, I have sustained and continue to sustain substantial injuries, which include, but are not limited to: financial loss, humiliation, embarrassment, severe mental and emotional distress, and discomfort, which encompass damages which total in excess of initial injuries caused by the monetary loss due to the monies that were transferred to the fraudsters.

#### LACK OF VIGILANCE

Rather than engage in any interactive processes you acted rashly and without prudence, and I was harmed as a result. Your failure to engage in good-faith interactive processes was, again, a substantial factor in causing harm to me. It has already been established that there are some situations where financial institutions should not have taken their customers' instruction at 'face value' -- and should have looked at the wider circumstances surrounding the transactions prior to authorizing their execution.

During the course of our relations, you failed to prevent me, as your customer, from engaging in such actions that resulted in my being subject to financial abuse and failed to introduce an adequate risk- based approach as set out by the applicable regulations and guidelines.

#### FURTHER POINTS FOR CONSIDERATION

It is well-established that a compensation obligation arises in the circumstances discussed above as contemplated by the standards, and that the regulated and licensed financial institutions, despite not having perpetrated the fraud themselves, should be uniquely placed in the role of an insurer, insofar as reasonable. Granted, the fraud has taken place entirely outside of the domain of the financial institution, nevertheless, both common sense and methodological approaches to problem-solving suggest that the financial institution should have had the investigative powers, the know-how, and the resources not only to detect this foreseeable fraud but also to discover the nature or merits of this claim, and when appropriate, reimburse the client. In the computer age, when access to technology and information is abundant, it is no longer exclusively a matter for law enforcement or government- led action. Moreover, it is better to seek to protect users, increase costs for users, and even limit choice, than to achieve a compromised protective environment and in doing so provide fertile ground for criminal organizations to flourish and enrich themselves.

Given that the recordings of all completed transactions on the Blockchain are publicly available, easily accessible, and fully transparent, for example, through <https://www.blockchain.com/>, it would be plausible to assert that you utterly failed to satisfy yourself that the cryptocurrencies were actually being sent to legitimate recipients — as it could have been easily verified and flagged thereafter. Furthermore, you should be aware of the tactics often utilized by fraudsters such as large movements of sums in short periods of time as well as thousands of micro-transactions which create a false sense of demand, tumblers, and mixers. You have routinely failed to exercise your clear, nondiscretionary, and indisputable duty to inquire and/or report if suspicious activities are involved in the movement of the digital funds; absent an appropriate set of inquiries as to the legitimacy and legality of the transactions, and as a result, fraudsters will continue to thrive.

#### FRAUD DETECTION SERVICES

It is clear that I was injured through the misconduct described above and was subject to the fraudsters' unfair and unlawful conduct. It is clear that any rational individual could have been deceived just as easily as I have been under the circumstances, hence I suggest you adapt yourself, as a respectable and resourceful financial institution, to the technologically rapid-changing financial service environment. If

you are serious about fighting crime, it is upon you to invest in fraud detection services, irrespective of whether or not it is expressly specified in the relevant regulatory requirements.

Fraud detection services are often predicated on non-PII data (Non-Personally Identifiable Information) thus not robbing individuals of their anonymity. Instead, they utilize digital footprints and behaviour analysis. It is expected of firms to take action within the existing legislative and regulatory framework to suspend or freeze payments based on their risk assessment managing the risks of financial crime. The standards that financial institutions need to meet would include processes – such as the use of technology, rules and procedures – that help prevent and respond to scams similar to the one described herein.

Scrutiny shows that the global internet community was fully cognizant of the Company's criminal nature during the relevant time-period. Nevertheless, it is plausible to assume that neither preventive nor proactive measures have been taken from your end to protect my financial interests.

Based on information and belief, Paxos, although being a regulated and licensed company (to the best of my knowledge) provides fertile ground for foreseeable financial abuse, wittingly or unwittingly promotes the flourishing of cyber-thieves, and aids and abets ICO and boiler room scammers in their commission of fraudulent acts by, among other things, not sufficiently scrutinizing the circumstances of client transactions; Given its enormous volumes of data and applications, cybersecurity capacities, human capital and know-how, Paxos does little to safeguard the financial interests of its clients.

#### CONCLUSION

If a full refund is not administered within 7 days from the date of this letter, in addition to a refund amount, a request for reimbursement of attorney's fees, filing fees, and any further costs associated with obtaining the refund amount may be pursued.

If despite the credibility of this claim, you do not take steps to shut down this lifeline to the fraudster's operation or to expose the illegal activities to law enforcement authorities, you are obviously directly participating in a fraud. No matter how inexplicable and suspicious these transactions were, you executed each and every transaction, thus unlawfully generating immense profits from a fraud. In order to perpetrate the fraud, the criminals needed a financial institution that would be friendly and hospitable to scammers, in other words, an institution which would blind itself to and overlook suspicious activity, completely ignore the grossly excessive activities in their accounts, and

conveniently ignore its obligations under the law. It was not reasonable during the time the transactions in question were executed, for you to believe that the transactions were a result of anything other than misappropriation of the funds, especially in light of the fact that you were fully aware, at the relevant time period, that such scams are prevalent and could have done more to spot it before the money was handed over.

In the event of non-compliance with the demand mentioned above, your organization, knowingly or unknowingly, manifestly jeopardizes its business through its association with the criminals: those who are not direct accomplices to the commission of a crime but rather are permissive of the criminal behavior after the crime has been committed can also be charged with a crime. Being permissive, even if not present when the crime was committed, by not reporting the crime to the authorities and not trying to do your part in remedying the situation, makes you an accessory to the crime. In accordance with moral law, if you unknowingly assist criminal behavior and remain impartial after discovering such, you are seen as obstructing justice.

This letter does not realize the full extent of my claims, rights, and remedies against you or any of your affiliates, parents and subsidiary corporations, including, without limitation, your representative managing partners, officers, directors, shareholders, employees, agents, attorneys, assigns, successors, servants, insurers, and representatives, in any matter whatsoever, including the present context of this letter, as that will not detract from my rights and claims in any form or manner whatsoever, or constitute any concessions on my behalf against you and against others.

For ease of reference, I have included transaction statements and warnings against the merchant. Sincerely,

(b)(6)

**File**

(b)(6)

**Incoming Complaint:**

From: (b)(6) (b)(6)@gmail.com]

Sent: 5/29/2023 12:30 AM

To: help@sec.gov

Subject: SÉC of ITBIT

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello! Good day everyone! May I ask if the ITBIT TRUST COMPANY,LLC is registered in SÉC?thank you!--  
Sent from Gmail Mobile

## **File**

(b)(6)

### **Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 8/12/2023

Origin: Web

File #: (b)(6) ~::HO

Send to Entity: Yes

#### **Investor Information**

Name: (b)(6)

Address: (b)(6)

(b)(6)

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6) @gmail.com

#### **Entity Information**

Name: Plynk

Type: Broker-Dealer

Representative: All involved and Other Partner Company logos audit

Address:

#### **Security Information**

Name: Plynk Paxos Plaid audit them. My account

Symbol:

Type: Currency transactions

#### **Description:**

Paxos crypto price fixing. You will 100% find that on this date probably others.

Time price analysis audit.

Stock securities probably the same. bid ask ECT...

**File**

(b)(6)

**Incoming Complaint – Phone call:**

Correspondent inquires about Paxos Trust Company; a subject connected to crypto

**File** (b)(6)

**Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 10/2/2023

Origin: Web

File #: (b)(6) ~::HO

Send to Entity: Yes

**Investor Information**

Name: (b)(6)

Address: (b)(6)

(b)(6)

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6)@hotmail.com

**Entity Information**

Name: Paxos Trust Company LLC

Type: Other

Representative: (b)(6)

Address: New York

, NEW YORK 10017

**Security Information**

Name: Paxos Trust

Symbol:

Type: Currency transactions

**Description:**

On December 31, 2019, BUSD tokens were issued to Paxos Trust Company and Circle Internet Financial the total amount in BUSD was (b)(6) which was denoted under my Ethereum smart contract, (b)(6) ----- (b)(6) and contract (b)(6) ----- (b)(6) on December 31, 2018, the total amount dated at the time (b)(6) as reported by Etherscan.

The USDC tokens that were issued and outstanding denoted under contract Circle is (b)(6) -----

(b)(6) and (b)(6) ----- (b)(6). I didn't submit the entire Contract ID just in case I need to keep it private.

I also have all the information you will need for proof, that these are my smart contracts. One of my main sources is GitHub.

my wallet info, private key and the independent account reports

Just a short history of why this was out there circulating on the blockchain. Back in 2016, I had purchased two smart mining contracts with Genesis-mining, unfortunately I lost my 12-letter recovery key, so was unable to get my daily



payout, I found my key and noticed from using EtherScan that my tokens were sent to Paxos and Circle, AND that the contract private key matches. mine

I have reached out to Paxos and Circle several times, wanting to know what's the procedure and what I need for proof to claim my Reserve Account, and not getting any directions everyone seems not to understand what I am talking about. So, I decided to take this route.

**File** (b)(6)

**Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 4/6/2024

Origin: Web

File #: (b)(6) ~::HO

Send to Entity: Yes

**Investor Information**

Name: (b)(6)

Address: (b)(6)

(b)(6)

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6)@me.com

**Entity Information**

Name: Paxos Trust Company, LLC

Type: Bank

Representative:

Address: 450 Lexington Ave., Suite #3952,

new york, NEW YORK 10163

**Security Information**

Name:

Symbol:

Type: Currency transactions

**Description:**

Dear SEC Team,

I am writing to report a distressing experience involving what appears to be a Ponzi multi-marketing scam.

Approximately two years ago, I fell victim to an investment opportunity presented by a friend, which led me to various websites promising wealth generation through currency exchange, notably M4Markets operating under aliases like FXTM. Despite initial investments, I faced insurmountable obstacles withdrawing funds, compounded by requests for additional investments.

The scheme involved platforms such as PAXOS, purportedly facilitating transactions but ultimately leading to financial losses. Notably, PAXOS operates within the US. Other affiliated websites, paxos allowed me to purchase bitcoin then to transfer those bitcoin to these overseas unregulated forex broker in different countries i did not know at the time including HTFX 4Markets, and other appeared interconnected, orchestrating false promises of wealth accumulation and learning courses and currency exchange.

I implore the sec to take immediate action to prevent further exploitation by these fraudulent entities. Additionally, I seek assistance in reversing my deposits to paxos that were over (b)(6) in chargess incurred on my Chase savings account. By exposing these fraudulent activities, we can safeguard others from enduring similar financial losses. When I spoke to Chase about the issue, they say there is nothing they can do. The email I have registered with Paxos (that's how they locate your account is (b)(6)@gmail.com).

Thank you for your attention to this matter. I await your prompt response and assistance.

**File**

(b)(6)

**Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 4/10/2024

Origin: Web

File #: (b)(6) ~::HO

Send to Entity: Yes

**Investor Information**

Name: (b)(6)

Address: (b)(6)

(b)(6)

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6)@mailfence.com

**Entity Information**

Name: paxos trust company

Type: Bank

Representative:

Address:

new york, NEW YORK

**Security Information**

Name:

Symbol:

Type: Bank issues (general)

**Description:**

i was victim of a fraud , i send several wires to paxos, to convert the money to their coin , then i was victim of a ponzi scam where i deposit those coins into their scammers platforms , i just found out that paxos was sued by the sec and order them to stop for for violating investor protection laws i submit the claims to chase (b)(6) . they say "We are processing the investigation for this wire under JPM Case ID (b)(6) . (last 2 digits of the other 5 wires) (b)(6) but also say these: Please be advised that we cannot action your request as beneficiary bank is already closed. We close our file.

can you please provide me feedback thank you

**File** (b)(6)

**Incoming Complaint – Phone call:**

Correspondent complains about Paxos Trust Company and a victim of an advance fee/ cryptocurrency scam involving Binance.

**File** (b)(6)

**Incoming Complaint:**

Correspondent Name: (b)(6)

Create Date: 3/7/2022

Origin: Web

File #: (b)(6) ~::HO

Send to Entity:

**Investor Information**

Name: (b)(6)

Address:

,

Day Phone: (b)(6)

Alt Phone:

Fax:

Email: (b)(6)@gmail.com

**Entity Information**

Name:

Type:

Representative:

Address:

,

**Security Information**

Name:

Symbol:

Type:

**Description:**

My question is: Can a broker withhold/freeze your deposited assets to ask arbitrary questions about assets you hold with other investment companies, and to challenge your investment strategy?

I am experiencing this right now with the Paxos financial institution.

I chose them as a digital asset / crypto exchange because they said they were regulated and transfer/trading costs were low.

I chose them, also, because they are partnered with Interactive Brokers, and as an existing customer of IBKRS, I considered the association with Paxos to mean they were reputable.

I am Canadian and I completed their KYC process and was granted an account. I wire transferred funds from my IBKRS account to my Paxos account to invest in digital assets.

They accepted my funding, and allowed me to trade USD for BTC. Then I attempted to move BTC to a personal wallet to access a different blockchain.

It would seem to me and to the functionality on Paxos exchange that this is perfectly legal. It was within their stated dollar volume limits. But without any prior requirements/information, they froze my assets and emailed a list of personal questions and asked for bank statements from other accounts.

First they said to confirm my identity, but after I provided, they changed the stated purpose, and said it was to support the dollar volume of my intended trading. I have never been required to provide either at my home bank in Canada, TD Bank nor IBKRS.

This was AFTER I initiated the transaction, and appeared arbitrary. I wonder if they suspect me of money laundering, which is ridiculous considering all the information I provided on their request.

They also, without providing information to state what was happening with my BTC have continued to hold it in limbo - neither returning it to my account ie not approving the transaction; nor processing the transaction to my other personal account.

I can't see where it is. Its neither in my account, nor has been transferred to my personal account. This is Day 3.

I have never been required to provide proof of funds in other bank and brokerage accounts to complete a transaction before.

I have asked for a phone number to speak to a representative of their company: they will not provide a number or name. "We don't support by phone." Their customer emails are not named.

Are these actions/ behaviours legal? This seems to go beyond KYC process for opening an account.

Can they force me to provide personal information after accepting my deposit, allowing a transaction to be initiated, and then to not return my assets, or provide information about them?

It is about (b)(6) they are controlling, arbitrarily.

Can someone provide information about whether Paxos is allowed to do this?

Thank you for any information you can provide.

Regards,

(b)(6)

**File**

(b)(6)

**Incoming Complaint:**

From: (b)(6) (b)(6)@gmail.com]

Sent: 7/12/2022 12:07 PM

To: help@sec.gov

Subject:

I paid (b)(6) for 1 Bitcoin,

When that's what 1 Bitcoin

Cost. Bought it threw PayPal I

Asked for my money when it was at (b)(6)

I made a PayPal wallet when that was introduced. At that point, I was at

(b)(6)

My request went out again for collection. Nothing?

Now it's at (b)(6)

I bought Bitcoin when it was (b)(6) as a present,

he cashed out at (b)(6)

Do you have any suggestions

On how to go about this?