William P. Suriano
General Counsel
[redacted]
legal@bitcoinofamerica.org

August 3, 2022

VIA EMAIL – regulations@dfpi.ca.gov

Commissioner Clothilde V. Hewlett
State Department of Financial Protection and Innovation
One Sansome Street
Suite 600
San Francisco, CA 94104-4428

RE: Invitation for Comments – Crypto Asset-Related Products and Services

Dear Commissioner Hewlett:

This letter responds to the "Invitation for Comments on Crypto Asset-Related Financial Products and Services Under the California Consumer Financial Protection Law" (the "Invitation"). In the Invitation, the State of California Department of Financial Protection and Innovation (the "DFPI") "formulated topics and questions to assist interested parties in providing input" into the anticipated rulemaking process. As General Counsel for SandP Solutions, LLC, d/b/a Bitcoin of America ("BOA"), I will address at least some of those topics and questions. BOA appreciates this opportunity to have input on these important issues and topics facing the industry. BOA management and its staff are more than willing to provide additional information, if needed.

Background of BOA

BOA deploys kiosks that look similar to conventional automated teller machines but which, for the most part, deliver cryptocurrencies to a digital wallet as directed by our customer in exchange for cash deposited into the kiosk. The cryptocurrency selected by the customer (*e.g.,* Bitcoin, Ethereum, Litecoin, Shibu Inu) is sent directly from BOA's digital wallet to the digital wallet address identified by the customer. BOA currently has approximately 2,500 kiosks deployed in over 30 states and is the fourth largest deployer of cryptocurrency kiosks in the country.

BOA is licensed as a Money Service Business with the Financial Crimes Enforcement Network ("FinCEN"). As such, BOA is subject to various rules and regulations, including the following:

1. The requirement of having Know Your Customer (KYC") and Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") policies;
2. The requirement of conducting an annual independent review of BOA's BSA/AML policies and their implementation, along with other aspects of its compliance program;
3. The requirement of conducting annual BSA/AML training of all BOA's employees;
4. The obligation to file Currency Transaction Reports ("CTRs") and Suspicious Activity Reports ("SARs") as required by federal law; and,
5. Periodic examinations under USCA, Title 31.

BOA has a full time Compliance Department with an experienced Compliance Officer, and experienced and well-trained Compliance Analysts. In short, BOA takes its compliance obligations very seriously and has devoted significant resources to insure it complies fully with all federal and other applicable laws.

BOA is not unique in the industry in this regard. In my experience, all the responsible kiosk deployers take compliance quite seriously and devote considerable resources to combatting frauds and scams.

BOA also has robust policies, procedures, and software designed to protect consumers from scams and frauds. Through an affiliated entity, BOA has developed its own software that is deployed on all BOA's kiosks. Our software developers work closely with BOA's Compliance Department to identify and combat frauds and scams in real time. In many cases, BOA can implement software changes in a matter of days as the tactics of scammers and fraudsters change and evolve.

When a customer begins a transaction at one of BOA's kiosks, that customer must first input information needed to establish an account. As the size of the transaction increases (up to the maximum of $15,000 per day), so do the KYC requirements. Any customer who fails to input the required information into the kiosk will not be able to proceed with a transaction. After the customer inputs his or her information, that information is verified through various databases to ensure the customer is not on any prohibited person list. In addition, software also correlates the customer's name, address, and telephone number to confirm everything matches. Again, this step is a fundamental KYC process that confirms the customer's identity. During the sign-up process, a camera in the kiosk takes a picture of the customer. That picture can be used to compare the customer's image to the customer's government issued identification. When the account verification process is completed, BOA's software automatically sends the customer a text message sent to the cell phone number registered by the customer and verified by BOA. That SMS says as follows, among other things:

> PLEASE NOTE: Law enforcement, the government (including the IRS and Social Security), banks, credit card and software companies, and others will not demand or

> direct you to purchase Bitcoin or some other cryptocurrency at this machine. If someone has told you that you must buy Bitcoin or other cryptocurrency at this machine – STOP and immediately call our Help Desk at (888) 502-5003.

BOA performs enhanced due diligence on customers whose accounts raise any red flags during the sign-up process. Until a customer is verified, that customer cannot trade on one of BOA's kiosks. As the customer proceeds through the process of purchasing cryptocurrency, BOA will also score the wallet address being used by the customer. If the wallet address scores above a set limit, the transaction cannot proceed, and the wallet address is blacklisted on BOA's system so that it cannot be used in any trade.

After a customer's account is verified, the customer is permitted to continue with a transaction. After deciding to buy cryptocurrency and deciding which cryptocurrency to purchase, and before the customer deposits any cash into the bill receptor on the kiosk, the customer is given a specific warning, a copy of which is attached as Exhibit A. If the customer says he or she is being directed by a third party to purchase cryptocurrency at the kiosk, then the transaction cannot proceed. If the customer confirms he or she is not being directed to purchase cryptocurrency at the machine and that the cryptocurrency is being purchased for the customer's own account, then the transaction is permitted to proceed to the next step.

The customer is then given another screen that provides additional warnings and acknowledgments requiring a positive check off. A copy of that screen is attached as Exhibit B. Among other things, for the transaction to proceed, the customer is required to check a box acknowledging that a transaction, once completed, cannot be reversed. The acknowledgment even defines what BOA means by a "completed" transaction.

BOA's software continues to monitor each transaction in real time generating alerts that go directly to BOA's Compliance Department. For example, any time a customer uses his or her account more than 250 miles away from where the customer created the account, BOA's Compliance personnel will receive an alert that must be manually cleared. BOA's software also detects when a customer attempts to create multiple accounts and prevents that from happening.

Daily, weekly, and monthly monitoring of transactions leads BOA's Compliance Department to freeze or deactivate accounts. If an account is frozen, it is usually because additional enhanced due diligence is required. A frozen account can be reactivated when BOA's Compliance Department is satisfied the customer has responded promptly to enhanced due diligence requests. Deactivated accounts cannot be reactivated.

BOA has a detailed Elder Financial Exploitation policy and procedure manual, and reports instances of Elder Financial Exploitation to the appropriate state and local authorities.

BOA's Compliance Department personnel are experienced in detecting subtle clues in customer accounts that could indicate a fraud or scam is in process. For example, seeing a relatively

small change in the use of language by a customer in communications with BOA can be a clue that the customer's account has been taken over by a scammer. BOA's Compliance personnel may refer a matter to Customer Service for BOA's Customer Service to contact the customer directly.

In addition to a Compliance Department, BOA maintains a robust Help Desk with experienced personnel to field any questions customers may have concerning their transactions. The Help Desk refers calls directly to other departments, including Compliance and Legal, as warranted.

BOA files CTRs and SARs whenever required under federal law. BOA also cooperates fully with law enforcement in responding to subpoenas and warrants and, in some cases, reporting potential criminal activity in real time without the need for legal process. Indeed, BOA conducts a remote training program for law enforcement. BOA also timely responds to any consumer reports filed with the CFPB or state consumer protection agencies.

BOA participates in the ATMIA Deployers' Forum, a national trade association, dealing with common issues, including issues of fraud, education, and standard practices. Participants in the deployers forum discuss combatting fraud and scams and the practices used by the participants in combatting them.

BOA continuously re-examines its compliance policies and procedures, updating them as circumstances dictate.

Topics

BOA believes that any consideration of additional regulation should take into account that BOA, like many of its peers, takes consumer scams and fraud seriously and expends considerable resources combatting it. BOA's experience has been that all responsible participants in this market have a similar commitment. With those things in mind, this letter will now address some of the topics raised in the Invitation.

Topic 1 – What steps should the DFPI take to better protect consumers from scams and frauds associated with crypto asset-related financial products and services?

and

Topic 2 – What steps should the DFPI take to improve consumer education and outreach for crypto asset-related financial products and services?

Topics 1 and 2 are integrally related and are dealt with together. BOA believes the single most important thing the DFPI can do to help prevent crypto-related frauds and scams is education, particularly of the more vulnerable elderly. Once a transaction is completed, it cannot be reversed, even if that transaction is generated as the result of a fraud or scam. The best way to

protect consumers is through prevention and the best way to prevent scams and frauds is through education.

Media (including conventional and social) should be used to warn consumers of the risks of purchasing cryptocurrencies and of common scams and frauds. Media can be targeted to specific groups and localities. Local authorities, as well as the DFPI, should be encouraged to leverage their connection to those in their communities to educate them about cryptocurrencies and the associated risks, particularly scams and frauds.

The DFPI could also help in law enforcement training. Law enforcement should be trained to deal with cryptocurrency scammers and fraudsters. In our experience, there is often a disconnect between the way cryptocurrencies work and the way law enforcement thinks they work. A better understanding of cryptocurrencies and how they are abused would help law enforcement understand how scammers can be detected and stopped.

BOA is also aware of inconsistencies in the sophistication of the anti-fraud policies and procedures of deployers of kiosks in the California market. The DFPI should consider meeting with cryptocurrency deployers to develop minimum standards of practice that each deployer would be required to meet to operate in the state and to encourage deployers to do likewise.

Topic 3 – What steps should the DFPI take to better ensure consumer protection in the offering and provision of crypto asset-related financial products and services?

The DFPI might be surprised how seriously the industry takes frauds and scams and how hard it is working to minimize them. The DFPI should routinely meet with deployers and others in the industry to discuss what is happening in the marketplace and what deployers are doing to prevent or minimize scams and frauds. Scams and frauds are highly adaptive. As soon as deployers effectively combat one scam or fraud, another appears. Moreover, consumers often are migrated by scammers to the company with the most lax compliance program. Bringing all deployers up to certain standards that are clear and adaptable will be useful and, BOA believes, will benefit both consumers and the entire industry.

BOA, and others in the industry, stand ready to assist in developing standard practices that will ensure more consistent scam and fraud detection and prevention.

Topics 4 through 6

BOA believes the input of others on these topics will provide better direction to the DFPI than anything BOA can add. BOA is primarily a seller and buyer of cryptocurrencies, not an investor. In addition, BOA does not mine cryptocurrencies.

Topic 7 – How should the DFPI strive to harmonize its regulatory approach to crypto asset-related financial products and services with federal authorities?

and

> **Topic 8 – In developing a comprehensive regulatory approach to crypto asset-related financial products and services, how should the DFPI work with other state financial regulators to promote a common approach that increases the reach of DFPI's consumer protection efforts and reduces unnecessary burdens, if any, on companies seeking to operate nationwide?**

BOA has long advocated for a uniform approach to deployers among state and federal agencies. Many of the issues BOA confronts are not unique to California, or any other state for that matter. Many deployers, like BOA, operate in multiple states and are met with confusing and sometime conflicting legislation and regulation.

For example, some states only regulate deployers if they fall within the category of a money transmitter and determine that peer-to-peer transmission is not money transmitting. Other states decline to regulate deployers based on a finding that cryptocurrency is not money within the meaning of their statutes. Others, like New York, have stablished special license requirements that apply to those in the deployer industry.

Using its influence, the DFPI could help promote uniform regulation and could lead states in accomplishing that end.

One point should be made here. Although it is extremely difficult to track given the nature of cryptocurrencies, BOA believes that many, if not most, scams and frauds originate outside the United States. In other words, sharing information with other states is not likely to increase the number of scammers who are caught. However, sharing may well help in preventing future scams and frauds and will help highlight those deployers who are not employing effective measures to combat scams and frauds.

> **Topic 9 – How can the DFPI make California the most desirable home state for responsible companies when developing guidance and, as appropriate, regulatory clarity and supervision of persons involved in the offering and provision of crypto asset-related financial products and services in California?**

BOA believes that clarity, consistency, and communication are all important to making California a desirable home for crypto asset-related financial products and services. The DFPI should recognize that companies like BOA have a large investment in both hardware and software. A stable, clear environment for this investment is always desirable. In addition, the DFPI should recognize that deployers like BOA are similarly concerned about scams and frauds. The industry, particularly the responsible companies, are more than happy to work with the DFPI and other state agencies to combat and prevent scams and frauds.

Overdoing it with oppressive regulation, however, will stifle further development of the industry in California. As noted below in response to Topic 10, the kiosk industry benefits certain groups traditionally underserved with financial services and products, including the unbanked and low-income investors. Excessive regulation will adversely impact those groups disproportionately.

> **Topic 10 – How should the DFPI ensure that California values of inclusive innovation and equity-based consumer protection are core components of crypto asset-related financial products and services as it develops guidance and, as appropriate, regulatory clarity and supervision of those persons involved in the offering and provision of crypto asset-related products and services in California?**

BOA prides itself on having a diverse work force. More importantly, by its nature, cryptocurrencies are available to a diverse community who may be unbanked or who have no access to what they consider to be "investment" opportunities that, in the past, would have been available only to the wealthy. Indeed, at one of BOA's kiosks, a consumer can purchase as little as $5.00 of Bitcoin per transaction. The existence of cryptocurrency kiosks has provided access to financial products and services that was not widely available to under-resourced communities in the past. In the future, kiosk providers like BOA can be expected to bring even more products and services to their kiosks, including things like bill payments, check cashing, debit cards, micro loans, and other financial products – all of which can be made available to under resourced communities.

Accessibility has to be balanced against the risks, but that is generally true in many financial products and services. Nonetheless, the ability of the unbanked and the small investor to go to a local gas station and purchase cryptocurrencies with the expectation those purchases will become more valuable as a future investment is unprecedented.

Questions

In addition to the above topics the Invitation posed a number of questions, some of which are answered below:

> **Question 11 – Are regulations needed to require registration of crypto asset-related financial products or services with the DFPI under Financial Code section 90009, subdivision (a) of the CFPL?**

and

> **What factors should be considered in determining whether the offer or provision of a crypto asset-related financial product or service should trigger registration?**

For the most past BOA simply sells cryptocurrencies that travel from its digital wallet to the digital wallet as directed by the customer. BOA believes these sort of peer-to-peer transactions do not and should not require any sort of product or service registration.

In addition, BOA and other deployers may begin to offer new services and products (e.g., bill payment, check cashing, etc.). These products and services are already regulated under other provisions of California law and BOA expects to comply fully whatever the regulatory requirements are for those services. BOA believes the existing regulatory scheme is sufficient.

Question 12 – Are regulations needed to specify crypto asset-related financial products and services that should be included in the definition of a "financial product or service" subject to CCFPL authority?

BOA does not believe additional regulations are required. If, for example, a cryptocurrency kiosk provider began offering Non-Fungible Tokens ("NFTs") through purchases made at a kiosk, there is an existing, adequate regulatory scheme for addressing the sale of NFTs. The same can be said of other products or services like check cashing.

Rather than developing an entirely new, parallel regulatory scheme, the DFPI could simply reference other regulatory schemes in place that deal with new services if and when they are made available. This will ensure consistency in the treatment of cryptocurrency kiosk deployers with others offering similar products and services, but in a more traditional, conventional manner.

Question 13 – Are regulations needed to identify any unlawful, unfair, deceptive, or abusive acts or practices in connection with the offering of crypto asset-related financial products or services?

BOA does not believe additional regulations are required. The existing framework for determining whether an act or practice violates the CCFPL is workable and adequate. Existing rulings and decisions related to the conduct addressed by the CCFPL provides sufficient guidance to cryptocurrency kiosk deployers without the need for additional regulations.

Questions 14 – Are regulations needed to ensure that features of crypto asset-related financial products and services are fully, accurately, and effectively disclosed?

This is an area where the DFPI could adopt regulations that would be helpful to both the consumer and the industry. When a customer purchases cryptocurrency at a kiosk, the customer may not know the fees the customer is paying. In addition, how those fees are calculated may vary from deployer to deployer. As a result, the consumer has no reasonable basis for comparing the fees of various deployers and selecting the deployer with the lowest acceptable fee.

Standardizing the way fees are calculated and what they consist of and then requiring them to be disclosed prior to a transaction being completed would be helpful to consumers and should not be objected to by the industry.

Question 15

A. Should the DFPI adopt rules requiring covered persons to file reports related [to] the offering and provision of crypto asset-related financial products and services? If so, what should such reports contain, and which report responses should be made publicly available?

B. Should the DFPI adopt rules requiring service providers to file reports related [to] the offering and provision of crypto asset-related financial products and services? If so, what would such reports contain, and which report responses should be made publicly available?

For kiosk deployers who trade peer-to-peer (*i.e.,* from the deployer's digital wallet to the wallet as directed by the customer), no reporting should be required. If a deployer engages in money transmission, there is already a regulatory framework for reporting that specifies what must be reported and what is made public.

BOA, and others in the industry, are on the front lines so to speak. Our collective experience should be prudently relied upon by the DFPI, as needed.

Question 16

A. Which companies should the DFPI include in the [market-monitoring] inquiry?

B. What products and services should be included in the inquiry?

C. What information, if any, should the DFPI collect and publish in the aggregate/

D. Should the DFPI publicly post its inquiry online and allow any company to voluntarily respond?

BOA believes the DFPI should post its inquiry online and allow any company to respond voluntarily. That will ensure the broadest scope and the widest representation of interests that could, in some cases, be missed if a narrower group were solicited.

Conclusion

BOA appreciates the DFPI's willingness to involve the industry in its consideration of future regulation. BOA is more than willing to provide additional insights, if requested.

Sincerely,

[redacted]

William P. Suriano

EXHIBIT A

AML SOFTWARE

Please Read

X

STOP!

Have you been contacted by any of the following?

- Law Enforcement (e.g., U.S. Marshal, Social Security Administration, or local police department)
- Computer technical support
- Bank/financial institution fraud department
- A third party asking you to purchase virtual currency

I have been instructed to buy virtual currency

I am purchasing virtual currency for myself

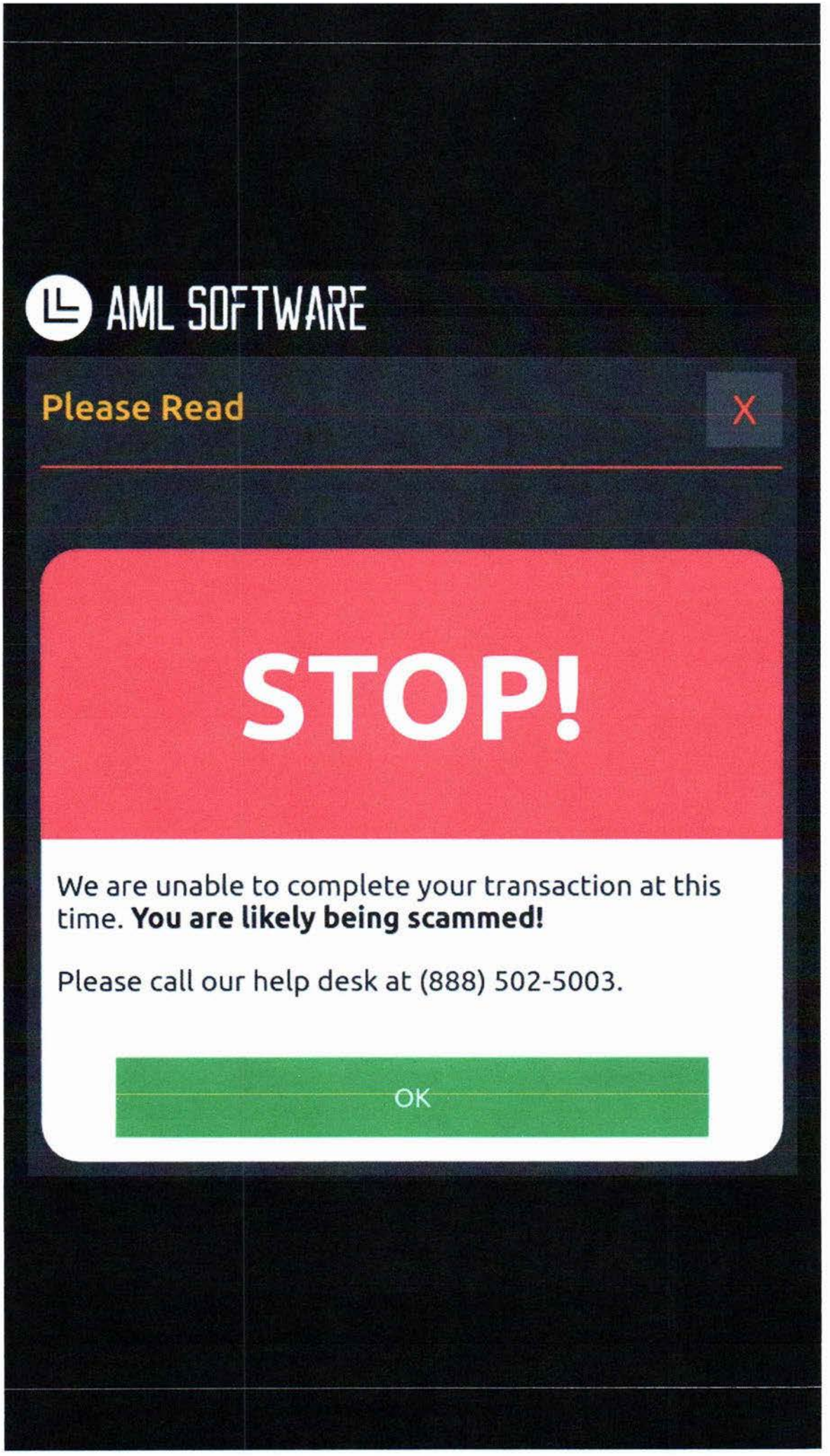
AML SOFTWARE
Please Read
X
STOP!
We are unable to complete your transaction at this time. You are likely being scammed!
Please call our help desk at (888) 502-5003.
OK

EXHIBIT B

bitcoin of america

YOU ARE BOUND TO THESE TERMS. YOU MUST AGREE AND CHECK THE BOXES TO PROCEED.

- [x] This account belongs solely to me, was opened by me with my own phone number, and is used or managed only by me.
- [x] I understand Bitcoin of America kiosk software can only be used to buy/sell virtual currency.
- [x] I understand I cannot access bank or depository accounts using Bitcoin of America software.
- [x] I understand once my trade is complete, i.e., I have paid for virtual currency and it has been sent to the wallet address I provide, it cannot be reversed.
- [x] I understand all of the above describe the intended use of Bitcoin of America's kiosk services.

I certify that the above is correct and true.

Click here to read the full Terms of Use ("Terms")

Cancel & return home.

I agree to the terms.