Response to Questions Regarding the Recent Incident

Investment Procedure:

Q: Did the xx Foundation send 1.5 million WXX without receiving any payment or counterpart before sending the coins?

A: The xx Foundation did send 1.5 million WXX coins without receiving any payment or counterpart before sending the coins. This occurred due to a Man-in-the-Middle (MITM) attack during the transfer process, which we explained in the recent update. Scammers impersonated foundation members, leading to the coins being transferred to an incorrect wallet controlled by the scammer. This incident was a result of social engineering, causing a breakdown in procedure and ultimately human error. It is important to note that the coins lost belonged to the xx Foundation, not individual community members. Some community members, who had limit purchase orders on Uniswap, were able to buy xx coins at lower prices during the incident. While this was a negative situation for the foundation, it provided an unintended opportunity for some community members to purchase coins at lower prices. This is not an attempt to spin for positivity; it is simply a fact.

Bridge and Security:

Q: Can individuals still bridge XX to WXX after the incident, and what measures are in place to secure these transactions?

A: The bridge was never compromised. When the scam happened, the Foundation acted immediately to shut down the xx/WXX bridge and informed the CEXs to shut down WXX pairings so that the scammer was cornered in Uniswap and could not sell the coins in higher liquidity markets. This is not an issue; the bridge remains secure.

Response and Verification:

Q: Were the real individuals impersonated by the scammers contacted separately to verify their identities using secure methods like PGP?

A: The nature of the MITM attack negated the fact that the impersonated people had verified their identities prior to the scam. It all happened in real time. The method

used was effective enough to trick our foundation members, although in hindsight it is easy now to see what was done wrong. This is why we are running an internal review and updating the foundation investments transfer procedure which must be followed to accommodate for the hard lessons that were learned with this unfortunate incident.

Q: What steps are being taken to track down and identify the scammer?

A: We will not telegraph our steps here. If the scammer were, for example, listening to this chat and we were explaining all of our steps to find them, it would signal to them what they should do to avoid detection. Please understand that given the level of sophistication they showed through the process, it will likely be difficult to find them. We are doing what we can.

General Questions:

Q: Who has access to the WXX contract?

A: The WXX contract is open-source and transparently available on Etherscan. The question of "access" doesn't apply in the traditional sense, as the contract is immutable and publicly visible. No hack occurred, and the contract's security remains intact.

Q: Who makes decisions on OTC deals and why?

A: Decisions on OTC deals are made collectively by the xx Foundation's board. This process involves careful consideration and is part of our capital-raising strategies. Specific individuals' names are not disclosed as these decisions are organizational, not personal.

Q: Why aren't decisions on OTC deals made public like in other major project foundations?

A: It is common practice in the industry to keep specific details of OTC deals confidential, especially regarding the identities of investors, unless they consent to disclosure. However, the funding earmarked for specific projects would have been mentioned had this particular investment been successful, and the community would have been made aware of the reasons in this case if consent was given and it was deemed appropriate to do so, much like the grant program outcomes. While some projects may share fundraising outcomes, they do so when it aligns with their strategic interests.

Q: How can tokens be sold OTC to non-institutional investors?

A: The xx Foundation has facilitated investments with both institutional and non-institutional investors, provided they meet KYC/AML requirements. This practice is standard in the industry and adheres to legal and regulatory frameworks.

Q: Why are deals being made on DEX when there is a native token?

A: There were no deals made on a DEX as part of this incident. The sale of WXX coins was part of the negotiation process, which is standard for such deals. However, it is possible the question refers to why WXX was used in the deal at all. This use of WXX was a final request in the negotiations, which the foundation accepted because it was technically feasible. However, we have learned from this situation that it is not in our best interest to add extra complexity like this into any deals. In the future, only xx native coins will be used in coin investments to avoid unnecessary procedural complexity.

Q: The WXX address initially received 5,000,000 tokens for DEX liquidity. How was this address used?

A: These tokens are xx Foundation funds. This allocation was made to support broader market engagement and was not derived from community, council treasury funds, or bridge fund. These liquidity funds will be topped up to reflect our stated goals when necessary although any xx coins that the Foundation wants to move from xx to wxx will now be done via the xx network bridge.

Q: How did the fraudster pose as a team member?

A: We have chosen not to disclose detailed information about the scam's execution to avoid exposing potential vulnerabilities. Our priority is protecting the integrity of our operations and preventing further incidents.

Q: If tokens are bought OTC, can they also be sold OTC?

A: The xx Foundation has never facilitated OTC selling deals. This question does not pertain directly to the incident in question, and we do not see it as relevant to the current discussion. That said, we currently have no such deals pending and have no intentions to facilitate them.

Q: Why did the market maker (MM) buy tokens, allowing the scammer to sell at a better price?

A: As clarified in our statement, the market maker did not actively prop up the price. The rapid nature of the scam left little time for any response.

Q: The MM maintained the price by buying tokens instead of waiting for the scammer to dump all tokens.

A: This statement is incorrect. The market maker did not maintain the price in this manner. The situation developed quickly, and the market maker's actions were not as described. The MM had a few orders on the market as they normally do. When the scammer initially sold into the market all the orders at the initial market prices were executed immediately along with nearly everyone in the uniswap pool. The MM bot then was shut down almost immediately to assess the situation. At the time there were clearly other wxx holders that proceeded to populate the order books with low priced purchase orders which the scammers continued to sell into until all of their wxx was sold off. As we explained previously, the average sell price was $0.0313

Q: Why not switch to a more experienced market maker with better exchange integration, like DWF Labs?

A: While we do not discuss specific contractual relationships publicly, we can assure you that we are continually evaluating our partnerships to ensure they align with our strategic goals. Any changes to our market-making strategies, or any other service vendors, will be communicated appropriately.