

From: [noticing@ra.kroll.com](mailto:noticing@ra.kroll.com)

Email subject: IMPORTANT – Notice of Kroll’s Security Incident Involving Claimant Data/Steps to Protect Yourself

Email body:

*In re: FTX Trading Ltd., et al.*, Case No. 22-11068  
United States Bankruptcy Court for the District of Delaware

Kroll Restructuring Administration (“Kroll”), the claims agent in the bankruptcy, has learned that it experienced a cybersecurity incident that compromised personal data of certain claimants. Kroll promptly contained and remediated the incident, reported it to law enforcement and is investigating this matter. Kroll has advised the court and the FTX debtors of the incident. This email provides important information that can help protect you against potential misuse of this information. We encourage you to read this email carefully.

#### What happened?

On or about Saturday, August 19, 2023, an unauthorized third party gained control of a mobile phone number belonging to an employee of Kroll. As a result, the unauthorized party accessed files in Kroll’s cloud-based systems, including files that contained your name, address, email address, and the balance in your FTX account. When Kroll became aware of the incident, it acted quickly to secure the impacted Kroll account and launched an investigation. There is no evidence that the attacker accessed any other Kroll accounts or systems. Moreover, Kroll did not maintain passwords to FTX accounts. This attack on Kroll did not affect any FTX systems or FTX digital assets.

The attacker might use this information in a further scam, for example, by sending phishing emails to trick you into providing sensitive personal information or access to your personal accounts, including but not limited to, cryptocurrency accounts, wallets or other digital assets, wherever they may be held.

While no action is necessary as to your FTX account as a result of this incident, you can help maintain the security of your accounts and digital assets by remaining vigilant and taking certain steps, including the following:

- Never share your passwords, seed phrases, private keys, and other secret information with untrusted individuals, applications, websites or devices.
- Always verify information that you receive from any other website about the FTX bankruptcy case or your claim by visiting the website of the Claims Agent, Kroll Restructuring Administration LLC: <https://restructuring.ra.kroll.com/FTX/> or contacting Kroll Restructuring Administration at [FTXquestions@kroll.com](mailto:FTXquestions@kroll.com).

The Court presiding over the FTX bankruptcy case (the United States Bankruptcy Court for the District of Delaware), Kroll, and FTX will never ask or require you to do any of the following in connection with the processing of bankruptcy claims or the distribution of FTX assets:

- Link a cryptocurrency wallet to a website or application
- Provide your seed phrase or private keys
- Download any software or use a particular wallet application
- Provide your password over email, text message, or over the phone
- Provide personal identifying information, such as your birthday or social security number, over email, social media or in any manner other than as described in a Court-approved process posted to Kroll Restructuring Administration's case website or the Court's docket

For more information on how to protect yourself from identity theft and fraud, please visit [FTXQuestions.kroll.com](https://FTXQuestions.kroll.com).

Please know that any distribution of FTX assets will only be at the time and in the manner established by the Court. Information about the Court's orders can be found at the website of the Claims Agent, Kroll Restructuring Administration LLC: <https://restructuring.ra.kroll.com/FTX/>.

If you have any questions, receive suspicious communications, or wish to verify the authenticity of communications that are purported to be from individuals associated with the FTX bankruptcy case, please contact: [FTXQuestions@kroll.com](mailto:FTXQuestions@kroll.com).