

SHERROD BROWN, OHIO, CHAIRMAN
JACK REED, RHODE ISLAND
ROBERT MENENDEZ, NEW JERSEY
JON TESTER, MONTANA
MARK WARNER, VIRGINIA
ELIZABETH WARREN, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
CATHERINE CORTEZ MASTO, NEVADA
TINA SMITH, MINNESOTA
KYRSTEN SINEMA, ARIZONA
JON OSSOFF, GEORGIA
RAPHAEL G. WARNOCK, GEORGIA
PATRICK J. TOOMEY, PENNSYLVANIA
RICHARD C. SHELBY, ALABAMA
MIKE CRAPO, IDAHO
TIM SCOTT, SOUTH CAROLINA
MIKE ROUNDS, SOUTH DAKOTA
THOM TILLIS, NORTH CAROLINA
JOHN KENNEDY, LOUISIANA
BILL HAGERTY, TENNESSEE
CYNTHIA M. LUMMIS, WYOMING
JERRY MORAN, KANSAS
KEVIN CRAMER, NORTH DAKOTA
STEVE DAINES, MONTANA

LAURA SWANSON, STAFF DIRECTOR
BRAD GRANTZ, REPUBLICAN STAFF DIRECTOR

United States Senate
COMMITTEE ON BANKING, HOUSING, AND
URBAN AFFAIRS
WASHINGTON, DC 20510-6075

July 27, 2022

Mr. Sundar Pichai
Chief Executive Officer
Alphabet Inc. and Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

In recent years, crypto trading platforms and exchanges have experienced a surge in popularity with millions of investors downloading mobile apps to trade and invest in digital assets. Millions of Americans use mobile apps to invest in unregulated digital assets, including cryptocurrencies. Crypto mobile apps are available to the public through app stores, including Google's Play Store. While crypto apps have offered investors easy and convenient ways to trade cryptocurrency, reports have emerged of fake crypto apps that have scammed hundreds of investors.

The Federal Bureau of Investigation (FBI) recently issued a warning about the proliferation of fake cryptocurrency mobile apps created by cyber criminals to defraud investors.¹ Cyber criminals have stolen company logos, names, and other identifying information of crypto firms and then created fake mobile apps to trick unsuspecting investors into believing they are conducting business with a legitimate crypto firm.² Alarming, far too many investors have fallen victim to such scams with losses exceeding \$42 million.³ According to the FBI, in one case, cyber criminals defrauded at least two dozen investors by creating a mobile app that used the name and logo of a real trading platform. Investors downloaded the app and deposited cryptocurrency in wallets. Ultimately, the app was a fake and the victims of the scam could not withdraw funds from their accounts.⁴

¹ *Cyber Criminals Create Fraudulent Cryptocurrency Investment Applications to Defraud US Investors*, Federal Bureau of Investigation (July 18, 2022) (<https://www.ic3.gov/Media/News/2022/220718.pdf>).

² *Cyber Criminals Create Fraudulent Cryptocurrency Investment Applications to Defraud US Investors*, Federal Bureau of Investigation (July 18, 2022) (<https://www.ic3.gov/Media/News/2022/220718.pdf>); *Beware New Crypto App Scams: FBI Says Investors Have Lost Millions*, CNN (July 19, 2022) (<https://money.com/fake-crypto-app-scams-fbi-warning/>); *Fake Crypto Apps Have Stolen Over \$42 Million from Investors in Under a Year Warns FBI—How to Stay Safe*, CNBC (July 21, 2022) ([https://www.cnbc.com/2022/07/21/fake-crypto-apps-have-stolen-millions-from-investors-says-fbi.html#:~:text=Although%20%E2%80%9Ccrypto%20winter%E2%80%9D%20is%20showing,be%20legitimate%20cryptocurrency%20investment%20platforms\);](https://www.cnbc.com/2022/07/21/fake-crypto-apps-have-stolen-millions-from-investors-says-fbi.html#:~:text=Although%20%E2%80%9Ccrypto%20winter%E2%80%9D%20is%20showing,be%20legitimate%20cryptocurrency%20investment%20platforms);) See also *He Believed Apple App Store was Safe. Then a Fake App Stole his Lifesavings in Bitcoin*, Washington Post (March 30, 2021) (<https://www.washingtonpost.com/technology/2021/03/30/trezor-scam-bitcoin-1-million/>).

³ *Cyber Criminals Create Fraudulent Cryptocurrency Investment Applications to Defraud US Investors*, Federal Bureau of Investigation (July 18, 2022) (<https://www.ic3.gov/Media/News/2022/220718.pdf>).

⁴ *Cyber Criminals Create Fraudulent Cryptocurrency Investment Applications to Defraud US Investors*, Federal Bureau of Investigation (July 18, 2022) (<https://www.ic3.gov/Media/News/2022/220718.pdf>).

While firms that offer crypto investment and other related services should take the necessary steps to prevent fraudulent activity, including warning investors about the uptick in scams, it is likewise imperative that app stores have the proper safeguards in place to prevent against fraudulent mobile application activity.

To better understand the measures your company is taking to prevent fraudulent activity in your app store, please respond to the following questions by August 10, 2022:

1. Describe the review process your company takes before approving crypto apps to operate in your app store. In your response, please provide the following information:
 - a. The factors or criteria used by your company to determine whether to grant approval to an app, including the steps your company takes to confirm the app seeking approval is a trusted and secure app.
2. Describe the steps your app store takes to prevent cryptocurrency apps operating in your app store from circumventing app store policies by transforming into phishing apps. In your response, please describe in detail the frequency to which your app store monitors apps to safeguard against fraudulent activity as well as the steps it takes to remove apps determined to be fraudulent.
3. Describe all the systems and processes your company has in place for people to report fraudulent apps.
4. Describe all actions your app store has taken to alert people about actual or potential fraudulent activity associated with cryptocurrency investment apps.
5. Since January 2020, has your app store coordinated or shared any actions or activities with other app stores related to the suspension or removal of fraudulent cryptocurrency apps? If so, please explain.

Thank you for your prompt attention to this request. Should you have any questions, please do not hesitate to contact my staff at (202) 224-7391.

Sincerely,



Sherrod Brown
Chairman