UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF THE CHAIR

February 6, 2024

The Honorable Patrick McHenry
Chairman
Committee on Financial Services
U.S. House of Representatives
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Bill Huizenga
Chairman
Subcommittee on Oversight and Investigations
U.S. House of Representatives
2232 Rayburn House Office Building
Washington, DC 20515

The Honorable French Hill
Chairman
Subcommittee on Digital Assets, Financial Technology, and Inclusion
U.S. House of Representatives
1533 Longworth House Office Building
Washington, DC 20515

The Honorable Ann Wagner
Chairman
Subcommittee on Capital Markets
U.S. House of Representatives
2350 Rayburn House Office Building
Washington, DC 20515

Dear Chairmans McHenry, Huizenga, Hill, and Wagner:

Thank you for your letter regarding the unauthorized access to the Securities and Exchange Commission's (SEC) @SECGov X.com account on January 9, 2024. I appreciate your taking the time to share your thoughts.

As your letter notes, on Tuesday, January 9, 2024, the SEC's @SECGov X.com account was accessed by an unauthorized party. The party gained access to the account shortly after 4:00 pm ET by obtaining control over the phone number associated with the account in an apparent "SIM swap" attack.[1] Based on staff's consultation with the SEC's telecom carrier, it appears that the unauthorized access to the phone number occurred via the telecom carrier, not via SEC systems. Once in control of the phone number, the unauthorized party reset the password for the @SECGov X.com account.

After accessing the @SECGov X.com account, the unauthorized party made one post at 4:11 pm purporting to announce the Commission's approval of spot bitcoin exchange-traded products. The party also made a second post at 4:13 pm stating "$BTC." Using the @SECGov

[1] SIM swapping is a technique used to transfer a person's phone number to another device without authorization, allowing the unauthorized party to begin receiving communications associated with the number, including those that allow them to access bank accounts, social media profiles, and more. *See* Microsoft, *What is SIM swapping & how does the hijacking scam work?* (January 5, 2023), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping.

X.com account, the unauthorized party also liked two posts by non-SEC accounts. The unauthorized party subsequently deleted the second post within a minute, but not the first post. Neither post was drafted by SEC staff, nor did SEC staff "like" the two liked posts.

Once aware of the incident, staff in the Office of Public Affairs posted to the official @garygensler X.com account at 4:26 pm, alerting the public that the @SECGov X.com account had been compromised, an unauthorized post was made, and the Commission had not approved the listing and trading of spot bitcoin exchange-traded products.

At 4:37 pm, staff deleted the first (and only remaining) unauthorized post on the @SECGov X.com account. At 4:42 pm, staff successfully made a new post on the @SECGov X.com account stating that the account had been compromised. Staff also un-liked the two "liked" posts. Staff also reached out to X for assistance in terminating the unauthorized access to the @SECGov X.com account. Based on information currently available, staff believe that X terminated the unauthorized access to the account by 5:30 pm.

While this activity was ongoing, SEC staff actively reached out to and began coordinating with appropriate law enforcement and federal oversight entities, including the SEC's Office of Inspector General, the Federal Bureau of Investigation, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. SEC staff also alerted the Commodity Futures Trading Commission to the incident and were in touch with staff from the Department of Justice to coordinate investigative steps. The SEC's Division of Enforcement also was informed soon after discovery of the incident.

SEC staff continue to assess the scope of the incident and coordinate with all of our law enforcement partners. Among other things, law enforcement is currently investigating how the unauthorized party got the carrier to change the SIM for the account and how the party knew which phone number was associated with the account. At present, SEC staff have not identified any evidence that the unauthorized party gained access to SEC systems, data, devices, or other social media accounts.

On Wednesday, January 10, 2024, the Commission voted to approve the listing and trading of a number of spot bitcoin exchange-traded products.[2] On Friday, January 12, 2024, I issued a public statement on the SEC's website providing information about the unauthorized access to the @SECGov X.com account.[3] On Monday, January 22, 2024, SEC staff issued an additional statement on the SEC's website with further information about the incident.[4]

---

[2] *See* Self-Regul. Organizations; Nyse Arca, Inc.; the Nasdaq Stock Mkt. LLC; Cboe Bzx Exch., Inc.; Ord. Granting Accelerated Approval of Proposed Rule Changes, As Modified by Amends. Thereto, to List & Trade Bitcoin-Based Commodity-Based Tr. Shares & Tr. Units, Release No. 99306 (Jan. 10, 2024), https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf.

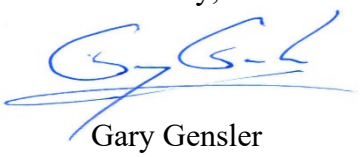
[3] *See* Statement on Unauthorized Access to the SEC's @SECGov X.com Account (Jan. 12, 2024), https://www.sec.gov/news/statement/gensler-x-account.

[4] *See* Statement by an SEC Spokesperson to the Media (Jan. 22, 2024), https://www.sec.gov/secgov-x-account.

I assure you that the SEC takes its cybersecurity obligations seriously. I understand that the SEC's Office of Legislative and Intergovernmental Affairs arranged a briefing on January 17 for your staff concerning the X incident and addressing the questions raised in your letter. SEC staff remains available to answer any additional questions you may have.

If you have any questions or comments, please feel free to contact me at 202-551-2100 or have your staff contact Kevin Burris, Director of the Office of Legislative and Intergovernmental Affairs, at 202-551-2010.

Sincerely,



Gary Gensler
Chair