DECLARATION OF SPECIAL AGENT CALEB ANDERSON

I, Caleb Anderson, Special Agent (SA) of the United States Secret Service (USSS), assigned to the Raleigh North Carolina Resident Office of the USSS, pursuant to 28 U.S.C. § 1746 and the laws of the United States, hereby declares under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This declaration is made in support of a complaint to forfeit funds previously seized from one bank account. This account contained proceeds from a business email compromise (BEC) fraud scheme, whereby one or more criminal fraudsters used deceptive tactics to gain unauthorized access to a business's email account. Once access was gained, the victim received am email requesting they send future payments to the subject account. A U.S. Magistrate Judge in the Eastern District of North Carolina previously issued a seizure warrant pursuant to 18 U.S.C. § 981(b) allowing traceable proceeds and other comingled funds involved in money laundering to be brought into government custody. I now submit this declaration to support the funds' forfeiture.

DECLARANT'S BACKGROUND AND EXPERIENCE

2. I am a Special Agent with the United States Secret Service (USSS) stationed in Raleigh, North Carolina and have been so employed since August 2021. I received criminal investigative training relevant to the subject areas addressed by the USSS at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. I am an investigative and

GOVERNMENT EXHIBIT A

law enforcement officer of the United States, in that I am empowered by law to execute warrants issued under the laws of the United States and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

3. In my official capacity as a Special Agent, I have personal knowledge of the information set forth in this declaration and/or obtained it directly from persons having knowledge of the facts of this case, including, as relevant, from speaking with or reviewing sources of information or other law enforcement personnel.

PURPOSE OF THE DECLARATION

4. I make this declaration in support of the civil forfeiture of the proceeds of a criminal scheme to defraud the North Carolina Housing Finance Agency (NCHFA) executed in violation of 18 U.S.C. § 1343 and co-mingled funds that were involved in the unlawful laundering of such property in violation of 18 U.S.C. § 1956 and 1957. Specifically, this declaration supports the civil forfeiture of the following asset: $2,767,919.94 contained in Currencycloud Inc. account XXXXXX6592 held in the name of FVB LTD that was previously seized and brought into government custody in September 2023.

BACKGROUND OF BUSINESS EMAIL COMPROMISES

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

6. A business email compromise (BEC) is a type of cyberattack where scammers use deceptive tactics to gain unauthorized access to a business's email account. This scheme typically involves impersonation of company executives or trusted individuals, sending fraudulent emails to employees, vendors, or clients. The deceptive fraudulent emails result in recipients disclosing

sensitive information, conducting wire transfers, or performing other actions that benefit the attackers. BEC attacks often involve social engineering and careful research to make the emails appear legitimate, making them a significant threat to businesses and their finances.

7. Scammers direct associates to open fraudulent business bank accounts (shell accounts) to facilitate the movement of BEC funds from the victims' accounts through one or more shell accounts before being distributed to the scammers orchestrating the scheme . Based off my training and experience, in these shell accounts, legitimate funds are not co-mingled, to include those funds used to open the account in furtherance of the crime.

FACTS SUPPORTING FORFEITURE

8. NCHFA, located at 3508 Bush Street, Raleigh, North Carolina, 27609, within the Eastern District of North Carolina, is a state agency that administers the Homeowners Assistance Fund (HAF), which falls under the federal American Rescue Plan Act. NCHFA has a contract with Innovative Emergency Management (IEM), which is a private company that assists NCHFA with the administration of North Carolina's HAF program. Occasionally, NCHFA sends HAF program funds to IEM, which in turn uses those funds to pay for housing expenses for applicants in danger of losing their home due to the COVID-19 pandemic.

9. On or about April 24, 2023, Steve Robinson, Network Intrusion Forensic Analyst (NIFA) with the USSS, located a complaint filed on April 20, 2023, by NCHFA on the Internet Crime Compliant Center (IC3) website. IC3 is a Federal Bureau of Investigations (FBI) website that serves as a reporting platform for victims of cyber-attacks. FBI provides IC3 access to all law enforcement (federal, state, and local) agencies for the ability to easily locate fraud victims. Based on the IC3 complaint filed by NCFHA, NIFA Robinson obtained the following information:

a. Two NCFHA employees in the financing department received emails requesting updates to the payment account for IEM. A controller at NCFHA requested a copy of a voided check for the new account, which was provided by the same sender requesting the updates. NCFHA initiated an approximately $2.7 million wire to the updated account for IEM.

b. Wells Fargo contacted NCFHA regarding the wire transaction, urging NCFHA to verify the account information with IEM. A representative at IEM advised the updates were not legitimate nor requested by IEM personnel. NCFHA realized the email address requesting the IEM account updates did not match other IEM employee email addresses, and subsequently, it was determined approximately $2.7 million had been wired to a fraudulent account.

10. Continuing on the same date, NIFA Robinson contacted NCHFA regarding the BEC and fraudulent transaction reported in the IC3 complaint.

11. NCFHA confirmed that on April 17, 2023, they received an email from an unknown subject posing as an employee of IEM, utilizing the email address "kent.barnett@iemmgt.com". NCFHA advised the fraudulent email was similar to the actual email address, "kent.barnett@iem.com", so NCFHA employees did not immediately notice the difference. The fraudulent email requested NCHFA update IEM's Automatic Clearing House (ACH) information, advising all future payments should be made to Community Federal Savings Bank account number XXXXXX6592.

12. On April 19, 2023, NCHFA initiated an ACH funds transfer from Wells Fargo Bank account XXXXXX1703 to Community Federal Savings Bank (Community Federal) account

number XXXXXX6592 in the amount of $2,767,914.18. The payment was conducted in accordance with the instructions provided in the previously mentioned fraudulent email.

13. On June 14, 2023, Community Federal responded to a USSS Raleigh Resident Office request, stating that a review of their [Community Federal's] databases revealed account number XXXXXX6592 was not a Community Federal account. Community Federal further advised the account number XXXXXX6592 was maintained by a bank customer, Currencycloud. As part of its business model, Currencycloud partners with Community Federal in order to conduct wire transfers and other transactions in states where Currencycloud is not directly licensed to conduct those transactions.

14. On July 17, 2023, Currencycloud provided financial documentation for account number XXXXXX6592, revealing that the account was opened on March 29, 2023 in the name of a United Kingdom-based business, FVB LTD, by a person named Florina-Victoria Constantinescu. The account was created through Silverbird Global Limited (Silverbird), which is an electronic money institution and acts as an earnest money deposit (EMD) Agent of Currencycloud, so payment or e-money services may be provided by Currencycloud. Financial documents confirmed the account received a payment of $2,767,914.18 on April 20, 2023. Currencycloud also received an invoice document from FVB LTD, in which FVB LTD claimed that they had billed NCHFA $2,766,530.22 for a "Consultancy and Management Fee". In addition to the fraudulent BEC payment of $2,767,914.18, the account received an initial funding deposit of 5.00 GBP (British pounds) on April 6, 2023. This 5.00 GBP was withdrawn to an external account on April 17, 2023. One other deposit of 5.40 Euros was also received in the account on April 11, 2023.

15. On 08/10/23, I applied for and was granted a warrant to seize the $2,767,914.18 in fraud proceeds contained in Currencycloud Inc account XXXXXX6592. I served the seizure warrant to Currenclycloud on August 11, 2023 and received $2,767,919.94 on September 21, 2023. The overage of $5.76 that was sent by Currencycloud is presumably the value of commingled funds (i.e., the 5.40 Euro deposit) that was utilized to fund the account and facilitate the laundering of the BEC fraud proceeds through said account.

CONCLUSION

16. Based on the foregoing, probable cause exists to believe that the entire $2,767,919.94 contained in Currencycloud Inc account XXXXXX6592, held in the name of FVB LTD, is subject to forfeiture to the United States pursuant 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 (Wire Fraud) or a conspiracy to commit such offense; and/or pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 or 1957. The funds to be seized represent proceeds of a business email compromise (BEC) scheme which involved the transmission of fraudulent emails by means of wire in interstate or foreign commerce, commingled with a nominal amount of other funds that were used to open and maintain this account for purposes of laundering criminally derived proceeds.

17. The foregoing facts are furthermore sufficient to support a reasonable belief that the defendant property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) and (C).

Executed this 24th day of January, 2024.

CANDERSON

Digitally signed by CANDERSON
Date: 2024.01.24 16:04:16 -05'00'

Caleb R. Anderson
Special Agent
United States Secret Service