

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term  
Grand Jury Sworn in on November 18, 2022

Case: 1:23-cr-00128  
Assigned To : Walton, Reggie B.  
Assign. Date : 4/18/2023  
Description: INDICTMENT (B)

UNITED STATES OF AMERICA

CRIMINAL NO.

v.

VIOLATIONS:

SIM HYON SOP,

18 U.S.C. § 1956(h)  
(Conspiracy to Launder Monetary  
Instruments)

Defendant.

FORFEITURE:  
18 U.S.C. § 982(a)(1);  
21 U.S.C. § 853(p)

**INDICTMENT**

The Grand Jury charges that, at times material to this Indictment:

**INTRODUCTION**

1. The charges alleged in this Indictment arise from an illicit scheme by North Korean Foreign Trade Bank (“FTB”) representative SIM HYON SOP (심현섭) (“SIM”), and others known and unknown to the Grand Jury, to launder proceeds generated by North Korean IT workers in violation of U.S. and UN sanctions against North Korea. These IT workers, who were based outside of the United States, used false identities to gain employment at U.S.-based and foreign blockchain development companies. Once hired, they asked for their salaries to be paid in virtual currency. The U.S.-based blockchain development companies made salary payments via their accounts at U.S.-based virtual currency exchanges. The IT workers and their co-conspirators, including SIM, employed a complicated scheme to launder the IT workers’ salaries to obfuscate the true beneficiary of their ill-gotten gains: North Korea.

2. Between in or around 2021, and up to and including on or about March 6, 2023, SIM, and by extension North Korea's FTB, received over \$24 million dollars' worth of laundered virtual currency, including at least \$12 million from IT worker revenue generation, in violation of U.S. sanctions against North Korea

### **ENTITIES AND INDIVIDUALS**

3. At all times relevant to this Indictment:

a. The Foreign Trade Bank of the Democratic People's Republic of Korea ("FTB"), headquartered in Pyongyang, North Korea, was North Korea's primary foreign exchange bank. FTB was a wholly state-owned institution that represented the government of North Korea in international, inter-bank communications. FTB maintained correspondent relationships with different financial institutions in many countries, and had offices in several regions of the world. FTB had more than 600 employees in its head office in Pyongyang, and approximately 300 employees worked in branches and subsidiaries. FTB performed functions for the North Korean government including, but not limited to, facilitating credit loans, making investments, regulating the use of foreign currency, setting the exchange rate for the North Korean Won, negotiating with foreign banks, facilitating foreign banking for North Koreans, buying and selling foreign currency, and facilitating the export and import of various commodities.

b. FTB was sanctioned by the UN Security Council and under U.S. law. Under U.S. law, the North Korean government, North Korean entities, or entities acting on behalf of North Korea were barred from access to the U.S. financial system.

c. Defendant SIM HYONG SOP was a North Korean national and resident of United Arab Emirates (UAE), who had no residence or last known residence in the United States, and who was employed by FTB to act as its representative in Dubai, UAE.



d. SIM's WALLET was an unhosted wallet address used by SIM and his co-conspirators to receive illegally obtained funds from IT workers deployed around the world, including funds originating from U.S.-based virtual currency exchanges.

e. VCE 1 was a global virtual currency exchange, with headquarters outside of the United States.

f. VCE 2 was a U.S.-based virtual currency exchange.

g. VCE 3 was a U.S.-based virtual currency exchange.

h. VCE 4 was a U.S.-based virtual currency exchange.

i. Victim Company A was based in the U.S. and maintained a virtual currency account at VCE 2 for business purposes.

j. Victim Company B was based in the U.S.

k. Victim Company C was based in the U.S. and maintained a virtual currency account at VCE 3 for business purposes.

l. Victim Company D was based in the U.S. and maintained a virtual currency account at VCE 4 for business purposes.

m. IT Worker B.C., who was based outside of the U.S., was hired by Victim Company A to complete IT development work and was paid in virtual currency via Victim Company A's account at U.S.-based VCE 2.

n. IT Worker J.P., who was based outside of the U.S., was hired by Victim Company A to complete IT development work and was paid in virtual currency via Victim Company A's account at U.S.-based VCE 2.

o. IT Worker A.H., who was based outside of the U.S., was hired (1) by Victim Company C to complete IT development work and was paid in virtual currency via Victim Company C's account at U.S.-based VCE 3; and (2) by Victim Company D to complete IT development work and was paid in virtual currency via Victim Company D's account at U.S.-based VCE 3.

p. IT Worker A.H., who was based outside of the U.S., was hired by Victim Company D to complete IT development work and was paid in virtual currency via Victim Company D's account at U.S.-based VCE 4.

q. VCE 1 Account A and VCE 1 Account B were accounts at VCE 1 obtained by SIM's co-conspirators through the false or fraudulent use of Russian identity documents. VCE 1 Account A and VCE 1 Account B were maintained by one of SIM's co-conspirators, a North Korean based in Russia, who used the accounts to send IT worker-generated funds to SIM's WALLET.

r. IT Worker J.P. VCE 1 Account was an account at VCE 1 obtained by the co-conspirators to be used in furtherance of this fraud scheme.

## The International Emergency Economic Powers Act and the North Korea Sanctions Program

4. The International Emergency Economic Powers Act (“IEEPA”), enacted in 1977, authorizes the President to impose economic sanctions in response to an unusual or extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat.

5. The Departments of the Treasury, Commerce, and State enforce and administer sanctions under their respective authorities. In particular, the Department of the Treasury publishes a publicly available list of individuals and entities (“Specially Designated Nationals and Blocked Persons” or “SDNs”) targeted by U.S. economic sanctions. SDNs’ property and interests in property, subject to U.S. jurisdiction or in the possession and control of U.S. persons, are blocked when they are placed on the SDN list. U.S. persons, including U.S. financial institutions, are generally prohibited from dealing with SDNs and their property and interests in property.

6. Using the powers conferred by IEEPA, the President and the Executive Branch have issued orders and regulations governing and prohibiting certain transactions with countries, individuals, and entities suspected of proliferating Weapons of Mass Destruction (“WMD”). On November 14, 1994, the President issued Executive Order 12938, finding “that the proliferation of nuclear, biological, and chemical weapons (‘weapons of mass destruction’) and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and [declaring] a national emergency to deal with that threat.”

7. On June 28, 2005, the President, to take additional steps with respect to the national emergency described and declared in Executive Order 12938, issued Executive Order 13382

(“Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters”) to target proliferators of WMD and their support networks and to deny designated proliferators access to the U.S. financial and commercial systems. Executive Order 13382 authorized the United States Secretary of the Treasury, in consultation with the Secretary of State, “to take such actions, including the promulgation of rules and regulations, as may be necessary to carry out the purposes” of the Executive Order. Pursuant to that authority, on April 13, 2009, the Secretary of the Treasury promulgated the “Weapons of Mass Destruction Proliferators Sanctions Regulations.” *See* 31 C.F.R. § 544.101 *et seq.* Executive Order 13382 and the Weapons of Mass Destruction Proliferators Sanctions Regulations prohibit transactions or dealings by any U.S. person or within the United States with individuals and entities placed on the SDN list, unless exempt or authorized by the Treasury Department’s Office of Foreign Assets Control (OFAC).

8. On March 15, 2016, the President, to take additional steps with respect to the previously described national emergency, issued Executive Order 13722 to address the Government of North Korea’s continuing pursuit of its nuclear and missile programs. Pursuant to that authority, on March 16, 2016, the Secretary of the Treasury promulgated the “North Korea Sanctions Regulations.” *See* 31 C.F.R. § 510.101 *et seq.* Executive Order 13722 and the North Korea Sanctions Regulations prohibit the export of financial services from the United States or by any U.S. person to North Korea, unless exempt or authorized by OFAC.

9. Executive Orders 13382 and 13722, the Weapons of Mass Destruction Proliferators Sanctions Regulations, and North Korea Sanctions Regulations also prohibit any transaction by any U.S. person or within the United States that evades or avoids, or has the purpose of evading or avoiding, any prohibition set forth in these regulations.

### North Korea's Foreign Trade Bank

10. On March 11, 2013, the Department of the Treasury designated the FTB, North Korea's primary foreign exchange bank, pursuant to EO 13382, for providing financial services that assisted in the proliferating of WMD. In the designation, Treasury stated, "North Korea uses FTB to facilitate transactions on behalf of actors linked to its proliferation network, which is under increasing pressure from recent international sanctions. . . . By designating FTB, the Treasury Department is targeting a key financial node in North Korea's WMD apparatus and cutting it off from the U.S. financial system. FTB is a state-owned bank established in 1959. FTB acts as North Korea's primary foreign exchange bank and has provided key financial support to [another designated entity, Korea Kwangson Banking Corp]." As a result of the designation, FTB was added to the Treasury Department's Specially Designated National ("SDN") List, which is published on OFAC's website.

### The Bank Secrecy Act

11. According to the U.S. Department of the Treasury, the global financial system, trade flows, and economic development rely on correspondent banking relationships. To protect this system from abuse, U.S. financial institutions must comply with anti-money laundering and countering the financing of terrorism requirements set forth in the Bank Secrecy Act (BSA), as well as sanctions and blocking programs administered by OFAC. The Treasury Department's Financial Crimes Enforcement Network (FinCEN) is responsible for administering the BSA in furtherance of its mission to safeguard the U.S. financial system. As is relevant to this Indictment, the BSA requires U.S.-based virtual currency exchanges to monitor activity on their networks and report to FinCEN, which is based in Washington, D.C., any suspicious activity, including activity involving, among other things, money laundering and financial crimes.

### North Korea's Deployment of IT Workers to Generate Revenue

12. Since in or around late 2017, North Korea has engaged in virtual currency-related thefts and fraud schemes to generate revenue for its ballistic missile and WMD programs. This virtual currency-related revenue generation has involved the deployment of IT workers to obtain illegal employment in the cryptocurrency industry. Specifically, North Koreans apply for jobs in remote IT development work without disclosing that they are North Korean. These IT workers bypass security and due diligence checks through the false or fraudulent use of identity documents and other obfuscation strategies, such as virtual private networks to hide their true location from online payment facilitators and hiring platforms. The IT workers request payment for their services in virtual currency and then send their earnings back to North Korea via, among other methods, FTB representatives such as SIM.

13. These IT workers are subordinate to North Korea's Munitions Industry Department ("MID"). MID is involved in key aspects of North Korea's missile program, including overseeing the development of North Korea's ballistic missiles, weapons production, and research and development programs. On or about August 30, 2010, OFAC designated MID as an SDN. On or about July 9, 2018, the UN sanctioned MID.

### Background Regarding Virtual Currency

14. Virtual Currency: Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not typically issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or BTC) and Ether (or ETH) are currently the most well-known virtual currencies in use.



15. Stablecoins: Stablecoins are a type of virtual currency pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. USD Tether (USDT) and USD Coin (USDC) are two stablecoins backed by the U.S. dollar.

16. Virtual Currency Address: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

17. Private Key: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

18. Virtual Currency Wallet: A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at one time. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

19. Blockchain: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. For example, BTC transactions are recorded on the BTC blockchain, and ETH transactions are recorded on the Ethereum network. A blockchain is

essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. A blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address.

20. Virtual Currency Exchange (VCE): VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. Many VCEs also store their customers' virtual currency in virtual currency wallets. These wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs qualify as "money services businesses" under the BSA (to the extent they operate "wholly or in substantial part within the United States"), they are legally required to conduct due diligence of their customers and to have anti-money laundering programs in place. *See* 31 CFR 1010.100(ff). A U.S.-based VCE is thus required to collect identifying information of their customers and to verify their clients' identities and to file reports with FinCEN regarding suspicious activity on their platforms. *See* 31 U.S.C. § 5311 *et seq.*

21. Decentralized Finance (DeFi): Decentralized Finance, or DeFi, is an umbrella term used to describe financial services offered on public blockchains, primarily the Ethereum network. DeFi is global, peer-to-peer, pseudonymous, and generally open to the public.

### THE CONSPIRACY

22. Beginning in or around 2021, and up to and including on or about March 6, 2023 (the "relevant time period"), SIM HYON SOP, together with others known and unknown to the Grand Jury, conspired to generate revenue for North Korea by laundering virtual currency obtained through illegal IT development work—some of which originated from U.S.-based virtual currency exchanges in violation of U.S. and UN sanctions against North Korea—and funneling those ill-

gotten gains using laundering mechanisms, such as accounts registered through the false or fraudulent use of identity documents, to transfer the virtual currency to North Korean-controlled accounts outside of the U.S., including SIM's WALLET. During the relevant time period, SIM, a North Korean FTB representative, and his co-conspirators created SIM's WALLET, which SIM used to receive over \$24 million in laundered virtual currency. At least \$12 million of that \$24 million was derived from illegal IT development work done for companies both inside and outside of the U.S.

***a. IT Worker B.C., IT Worker J.P., and IT Worker A.H. Obtained Illegal Employment at U.S.-based Companies***

23. In or around 2021, IT Worker B.C. and IT Worker J.P. obtained illegal employment at Victim Company A and asked to be paid for their work in virtual currency. IT Worker B.C. asked to be paid via IT Worker B.C. Address, and IT Worker J.P. asked to be paid via IT Worker J.P. Address. Victim Company A made those payments in USDC through Victim Company A's account at U.S.-based VCE 2.

24. To obtain employment at Victim Company A, IT Worker J.P. provided to Victim Company A records that falsely provided a particular address in the U.S. as his residential address; however, that address was actually associated with a restaurant.

25. In or around 2021, IT Worker J.P. obtained illegal employment at Victim Company B using fraudulently obtained identity documents of a U.S. citizen to legitimize IT Worker J.P.'s online persona.

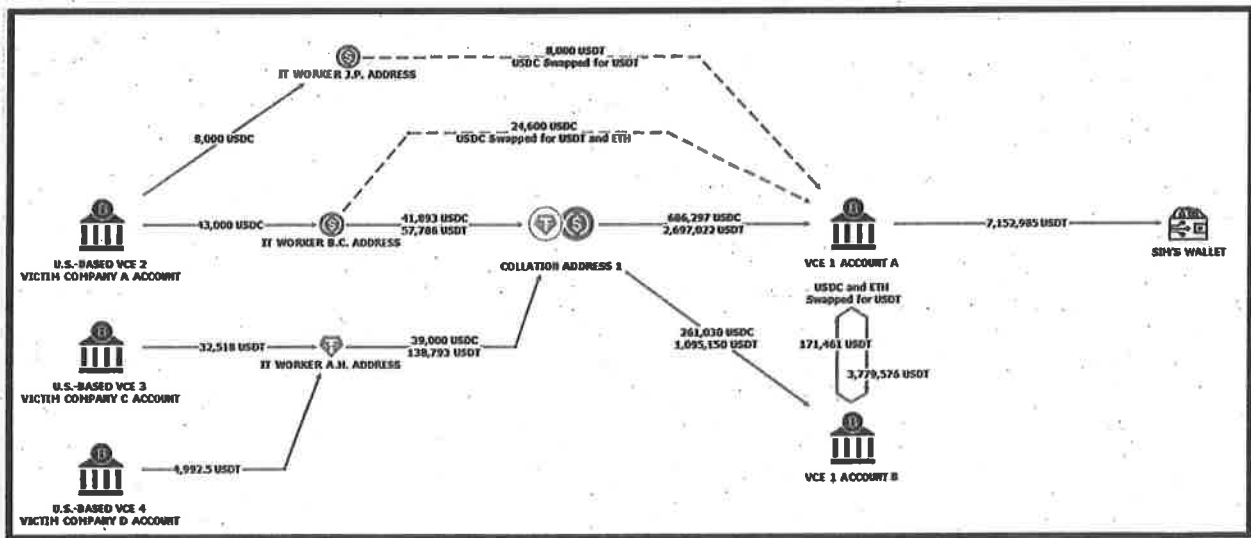
26. In or around 2021, IT worker A.H. obtained illegal employment at Victim Company C and Victim Company D. IT Worker A.H. asked to be paid by Victim Company C and Victim Company D via IT Worker A.H. Address. Victim Company C and Victim Company D made those payments in USDT using their accounts at U.S.-based VCE 3 and U.S.-based VCE 4, respectively.

**b. The Co-conspirators Caused Virtual Currency to Be Laundered and Sent to SIM's WALLET**

27. Ultimately, the co-conspirators caused those USDC and USDT payments, which originated in the U.S. at VCE 2, VCE 3, and VCE 4, to be laundered and eventually sent to accounts at VCE 1, including VCE 1 Account A and VCE 1 Account B. VCE 1 Account A and VCE 1 Account B were controlled by a North Korean co-conspirator based in Russia. That co-conspirator located in Russia used those accounts to send over \$7 million to SIM's WALLET.

28. During the relevant time period, IT Worker B.C. and his co-conspirators opened an account at VCE 1 (IT Worker B.C. VCE 1 Account) and used that account to send illegally obtained funds to VCE 1 Account A. The co-conspirators also caused illegally obtained funds to be sent directly from IT Worker B.C. VCE 1 Account to SIM's WALLET.

29. The above-referenced transactions, which originate from U.S.-based VCE 2, U.S.-based VCE 3, and U.S.-based VCE 4, are depicted in the graphic depicted below:



**c. SIM Sent at Least \$3.3 Million from SIM's WALLET to an Account at VCE 1 Controlled by SIM**

30. During the relevant time period, SIM caused at least \$3.3 million in virtual currency to be sent from SIM's WALLET to an account controlled by SIM at VCE 1. SIM and his co-

conspirators established that account at VCE 1 through the false or fraudulent use of identity documents, and registered the account using SIM's phone number. Additionally, those false, or fraudulently obtained, identity documents were stored within accounts controlled by SIM.

31. After sending at least \$3.3 million from SIM's WALLET to SIM's account at VCE 1, SIM and his co-conspirators used SIM's account at VCE 1 to convert the illegally obtained virtual currency to USDT. SIM and his co-conspirators sent that USDT back to SIM's WALLET as part of their laundering scheme.

**COUNT ONE**  
**(Conspiracy to Launder Monetary Instruments)**

32. The allegations set forth in paragraphs 1 through 31 of this Indictment are re-alleged and incorporated herein.

33. From at least in or around 2021, and up to and including in or around 2023, beginning out of the jurisdiction of any particular States or district and, pursuant to 18 U.S.C. § 3238, within the venue of the United States District Court for the District of Columbia, and continuing within the jurisdiction of the District of Columbia, pursuant to 18 U.S.C. § 3237(a), SIM, together with other co-conspirators known and unknown to the Grand Jury, did knowingly and willfully combine, conspire, confederate and agree to commit offenses against the United States, in violation of:

34. Title 18, United States Code, Section 1956(a)(2)(A), by transporting, transmitting, and transferring, and attempting to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, the export of financial services from the United States to an SDN in North Korea without having first obtained the required license from

OFAC, located in the District of Columbia, in violation of Title 50, United States Code, Sections 1702 and 1705; the Weapons of Mass Destruction Proliferators Sanctions Regulations, pursuant to Title 31, Code of Federal Regulations, Section 544.201, *et seq.*; and North Korea Sanctions Regulations, pursuant to Title 31, Code of Federal Regulations, Section 510.201, *et seq.*; all in violation of Title 18, United States Code, Section 1956(h).

### ***Goals of the Conspiracy***

35. The goals and purposes of the conspiracy were, among others:
- a. to generate revenue for North Korea's ballistic missile and WMD programs;
  - b. to access the U.S. financial system in violation of U.S. and UN sanctions against North Korea;
  - c. to prevent financial institutions and U.S.-based employers from verifying the true identity of North Korean IT workers;
  - d. to leverage the relative stability of virtual currencies backed by the U.S. dollar (*i.e.*, stablecoins, such as USDT and USDC) to avoid price volatility in the virtual currency market; and
  - e. to launder funds in the form of virtual currency in order to transact quickly and across multiple borders and jurisdictions.

### ***Manner and Means***

36. It was further a part of the conspiracy that SIM and his co-conspirators used the following manner and means, among others, to achieve the goals of the conspiracy:
- a. The co-conspirators used false, or fraudulently obtained, identity documents to obtain illegal employment at Victim Company A, Victim Company B, Victim Company C, and Victim Company D.

- b. The co-conspirators provided Victim Company A, Victim Company C, and Victim Company D with unhosted wallet addresses for payment in stablecoins, such as USDT and USDC.
- c. The co-conspirators caused Victim Company A, Victim Company C, and Victim Company D to send payments from their U.S.-based accounts to North Korean IT workers based outside of the U.S.
- d. The co-conspirators concealed FTB's involvement in the receipt of these illegally obtained funds by failing to reveal that North Korea was the ultimate beneficiary of income generated by, among other IT workers, IT Worker B.C., IT Worker J.P., and IT Worker A.H.
- e. To avoid law enforcement detection, the co-conspirators used the following laundering and obfuscation techniques, among others:
  - i. The co-conspirators sent their ill-gotten gains, in a rapid fashion, through a series of small transactions.
  - ii. The co-conspirators separated and then commingled their ill-gotten gains in unhosted wallet addresses.
  - iii. The co-conspirators obtained accounts at VCEs, including, but not limited to, VCE 1, using false, or fraudulently obtained, identity documents and then used those accounts to collate their ill-gotten gains.
  - iv. One of SIM's co-conspirators, who was a North Korean based in Russia, used VCE 1 Account A and VCE 1 Account B, which were both created using false, or fraudulently obtained, identity documents, to send their ill-gotten gains to SIM's WALLET.

- v. The co-conspirators converted their ill-gotten gains from one form of virtual currency to another.
- vi. The co-conspirators used accounts at U.S.-based professional networking platforms to legitimize their activities.

**(Conspiracy to Launder of Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h))**

**FORFEITURE ALLEGATION**

37. The allegations contained in Count One of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 982(a)(1). Pursuant to Title 18, United States Code, Section 982(a)(1), upon conviction of the offense alleged in Count One, violation of Title 18, United States Code, Section 1956(h), Defendant shall forfeit to the United States of America any property, real or personal, involved in such offense, and any property traceable to such property. The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, which constitutes, or is derived from proceeds traceable to this offense.

38. If any of the property described above, as a result of any act or omission of the Defendants:


- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,



the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

A TRUE BILL

FOREPERSON

  
Attorney of the United States in  
and for the District of Columbia