

1 RANDY S. GROSSMAN
Acting United States Attorney
2 OLEKSANDRA Y. JOHNSON
California Bar No. 265442
3 AARON P. ARNZEN
California Bar No. 218272
4 Assistant United States Attorneys
Office of the U.S. Attorney
5 880 Front Street, Room 6293
San Diego, CA 92101
6 Telephone: (619) 546-9769 (Johnson) -8384 (Arnzen)

7 Attorneys for Plaintiff
8 United States of America

9 **UNITED STATES DISTRICT COURT**
10 **SOUTHERN DISTRICT OF CALIFORNIA**

11 UNITED STATES OF AMERICA,

12 Plaintiff,

13 v.

14 Approximately 3879.16242937 bitcoin,
seized from Bitcoin address
15 bc1q7rhc02dvhmlfu8smywr9mayhdph85jl
pf6paqu,
16

17 Defendant.

Case No. '21CV2103 AJB JLB

COMPLAINT FOR FORFEITURE

18
19 By way of complaint against the Defendant, Approximately 3879.16242937 bitcoin,
20 seized from Bitcoin address bc1q7rhc02dvhmlfu8smywr9mayhdph85jlpf6paqu
21 (“Defendant” or “Defendant BTC”), Plaintiff, UNITED STATES OF AMERICA alleges:

22 **I. NATURE OF THE ACTION**

23 1. This is a civil action in *rem* brought against the Defendant to forfeit the
24 Defendant to the United States, pursuant to Title 18, United States Code, Section
25 981(a)(1)(C). In support thereof, Plaintiff alleges the Defendant BTC is subject to
26 forfeiture as property that constitutes or was derived from proceeds traceable to violations
27 of Title 18, United States Code, Sections 1343 (wire fraud) and 2314 (transferring or
28 transmitting in foreign commerce money that was stolen or taken by fraud). Each of those

1 crimes constitutes “specified unlawful activity,” as defined in Title 18, United States Code,
2 Section 1956(c)(7), including cross-reference to Title 18, United States Code, Section
3 1961(1)(B).

4 2. The Defendant BTC is also subject to forfeiture under Title 18, United States
5 Code, Section 981(a)(1)(A) as property that was involved in money laundering transactions
6 committed in violation of Title 18, United States Code, Section 1956 (Laundering
7 Monetary Instruments); and Title 18, United States Code, Section 1957 (Transacting in
8 Criminal Proceeds).

9 3. Title 18, United States Code, Section 981(a)(2)(A) defines “proceeds,” for
10 cases involving unlawful activities, as “property of any kind obtained directly or indirectly,
11 as the result of the commission of the offense giving rise to forfeiture, and any property
12 traceable thereto, and is not limited to the net gain or profit realized from the offense.”

13 **II. JURISDICTION AND VENUE**

14 4. This Court has original jurisdiction of this civil action under Title 28,
15 United States Code, Section 1345 because it has been commenced by the United States,
16 and under Title 28, United States Code, Section 1355(a), because it is an action for the
17 recovery and enforcement of a forfeiture under an Act of Congress.

18 5. Venue is proper pursuant to Title 28, United States Code, Section 1355(b)
19 because acts and omissions giving rise to this forfeiture action occurred in the Southern
20 District of California, and under Title 28, United States Code, Section 1395, and because
21 the Defendant property is located within the district.

22 **III. PARTIES**

23 6. Plaintiff is the United States of America.

24 7. Defendant is Approximately 3879.16242937 bitcoin, seized from Bitcoin
25 address bclq7rhc02dvhmlfu8smyw9mayhdph85jlpf6paqu, a Bitcoin address controlled
26 by an individual named Rei Ishii. The Defendant BTC was seized pursuant to a seizure
27 warrant issued by the Honorable Mitchell D. Dembin, United States Magistrate Judge for
28 the Southern District of California, in Matter # 21MJ2528.

1 8. The Defendant BTC is now located in FBI-San Diego's bitcoin wallet, in the
2 Southern District of California.

3 **IV. OTHER RELEVANT INDIVIDUALS AND ENTITIES**

4 9. Rei Ishii, also known as "Ray Ishii," is a former employee of Sony Life
5 Insurance Company Ltd. ("Sony Life"). Ishii is a dual national of the United States and
6 Japan.

7 10. Sony Life is an indirect subsidiary of Sony Group Corporation ("Sony
8 Group"), the Japanese multinational conglomerate. Sony Life is based in Japan.

9 11. Silvergate Bank is a Federal Reserve member bank based in La Jolla,
10 California, and is a financial institution, as defined in Title 31, United States Code, Section
11 5312(a)(2).

12 12. Coinbase, Inc., the company that operates Coinbase and Coinbase Pro in the
13 United States, is registered as a Money Services Business with the United States Treasury's
14 Financial Crimes Enforcement Network and is a financial institution, as defined in Title 31,
15 United States Code, Section 5312(a)(2).

16 **V. BACKGROUND ON BITCOIN**

17 13. Bitcoin¹ is a type of virtual currency, circulated over the Internet. Bitcoin are
18 not issued by any government, bank, or company, but rather are controlled through
19 computer software operating via a decentralized, peer-to-peer network. Bitcoin is one of
20 many varieties of virtual currency.

21 14. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address
22 is somewhat analogous to a bank account number and is represented as a 26-to-35-
23 character-long case-sensitive string of letters and numbers. Each Bitcoin address is
24 controlled using a unique corresponding private key. This key is the functional equivalent
25

26 ¹ Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted
27 practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol,
28 software, and community, and "bitcoin" (with a lowercase letter b) to label units of the
currency. That practice is adopted here.

1 of a password, or PIN, and is necessary to access the funds associated with a Bitcoin
2 address. Only the holder of an address' private key can authorize transfers of bitcoin from
3 that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at
4 any given time and may use a unique Bitcoin address for each and every transaction.

5 15. To acquire bitcoin, a typical user purchases them from a virtual currency
6 exchange. A virtual currency exchange is a business that allows customers to trade virtual
7 currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars,
8 Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging
9 traditional payment methods and virtual currencies) or online businesses (exchanging
10 electronically transferred money and virtual currencies). Virtual currency exchanges doing
11 business in the United States, including Coinbase, are financial institutions regulated under
12 the Bank Secrecy Act and must collect identifying information about their customers and
13 verify their clients' identities.

14 16. Individuals can send and receive cryptocurrencies through peer-to-peer digital
15 transactions or by using a third-party broker. Such transactions can be done on many types
16 of computers, including laptop computers and smartphones. To transfer bitcoin to another
17 Bitcoin address, the sender transmits a transaction announcement, which is electronically
18 signed with the sender's private key, across the peer-to-peer Bitcoin network. To complete
19 a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's
20 own private key. This information on its own rarely reflects any identifying information
21 about either the sender or the recipient. As a result, little-to-no personally identifiable
22 information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once
23 the sender's transaction announcement is verified by the network, the transaction is added
24 to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The
25 blockchain logs every Bitcoin address that has ever received bitcoin and maintains records
26 of every transaction for each Bitcoin address.

27 17. While a Bitcoin address owner's identity is generally anonymous within the
28 blockchain (unless the owner opts to make information about the owner's Bitcoin address

1 publicly available), investigators can often use the blockchain to identify the owner of a
2 particular Bitcoin address. Because the blockchain serves as a searchable public ledger of
3 every Bitcoin transaction, investigators can trace transactions to, among other recipients,
4 Bitcoin exchangers. Because Bitcoin exchangers generally collect identifying information
5 about their customers, as discussed above, subpoenas or other appropriate legal process
6 submitted to exchangers can, in some instances, reveal the true identity of an individual
7 responsible for a Bitcoin transaction.

8 18. The storage of bitcoin is typically associated with individual “wallets,” similar
9 to a virtual account. Wallets can interface with blockchains and generate and/or store
10 addresses and private keys. Exchangers and users of cryptocurrencies store and transact
11 their cryptocurrency in a number of ways, as wallets can be housed in a variety of forms,
12 including on a tangible, external device (“hardware wallet”); downloaded as software
13 (“software wallets”) on a personal computer or server (“desktop wallet”) or an application
14 on a smartphone (“mobile wallet”); as printed public and private keys (“paper wallet”); and
15 as an online account associated with a cryptocurrency exchange. Many users often back
16 up their virtual currency wallets using “recovery seeds.” A recovery seed, also known as
17 a root key, seed phrase, or recovery phrase, is a list of words that when entered in a specific
18 order into virtual currency wallet software, allows whoever is in possession of the words
19 to recreate access to virtual assets within the wallet.
20 Additional security safeguards for cryptocurrency wallets can include two-factor
21 authorization (such as a password and a phrase).

22 **VI. OVERVIEW OF REI ISHII’S CRIMES GIVING RISE TO FORFEITURE**

23 19. After acquiring two other insurance companies, Sony Life initiated several
24 transactions to exchange large sums of Japanese Yen for U.S. Dollars, and to transfer those
25 funds from a Citibank account in Bermuda to bank accounts Sony Life held in Japan.

26 20. Beginning no earlier than December 15, 2020, and continuing through at least
27 May 27, 2021, Rei Ishii (“Ishii”), who was one of the Sony Life employees responsible for
28 conducting those currency-exchange and fund-transfer transactions for Sony Life, engaged

1 in a scheme to defraud Sony Life, Citibank, and others, in connection with those
2 transactions. Ishii engaged in that scheme with the intent to surreptitiously and unlawfully
3 convert to his own use some of the Sony Life funds that were the subject of these
4 transactions. Ishii's fraud and embezzlement scheme involved material misrepresentations
5 and the concealment of material facts.

6 21. Between on or about May 18 and May 20, 2021 and as a part of this scheme,
7 Ishii obtained by fraud and embezzled approximately \$154,932,103.17 in funds belonging
8 to Sony Life.

9 22. Falsely, fraudulently, and without Sony Life's authorization, Ishii instructed
10 Citibank, one of the banks facilitating the May 18-20 transaction, to transfer
11 \$154,932,103.17 from a Sony Life Citibank account in Bermuda to an account that Ishii
12 controlled at Silvergate Bank in La Jolla, California, within the Southern District of
13 California.

14 23. The Silvergate Bank account to which Ishii directed those \$154,932,103.17 in
15 funds, which Ishii had obtained by fraud and embezzlement, is associated with Coinbase,
16 Inc. ("Coinbase"), a cryptocurrency company.

17 24. As a part of his scheme to defraud Sony Life, Ishii opened that Coinbase
18 account associated with the Silvergate Bank account on the materially false and fraudulent
19 representation, which involved use of international and interstate wires, that the account
20 belonged to Sony Life's subsidiary, SA Reinsurance, and that Ishii's supervisor, K.Y., was
21 the individual associated with the account.

22 25. Ishii then engaged in money laundering transactions involving the
23 \$154,932,093.17 in proceeds of his fraud and embezzlement scheme. Specifically, Ishii
24 caused Coinbase to exchange the \$154,932,093.17 on deposit at Silvergate Bank for
25 approximately 3,879.16 bitcoin cryptocurrency and then to transfer that corresponding
26 bitcoin to a secure and encrypted "cold wallet" having the address
27 bc1q7rhc02dvhtmlfu8smywr9mayhdph85jlpf6paqu, which belonged to Ishii, all knowing
28 that those transactions were designed in whole or in part to conceal the nature, location,

1 source, ownership, and control of those proceeds of his fraud and embezzlement crimes.
2 (The \$10 reduction in the amount of funds described herein, on information and belief,
3 reflects transaction fees.)

4 26. On or about December 1, 2021, with the assistance of Japanese law
5 enforcement authorities, the United States Federal Bureau of Investigation seized the
6 Defendant 3879.16242937 BTC and transferred it to FBI-San Diego's bitcoin wallet,
7 located in the Southern District of California. The Defendant 3879.162937 BTC reflects
8 the approximately 3,879.16 bitcoin transferred from Ishii's Coinbase account, as alleged
9 above, less network transaction fees.

10 **VII. FACTS OF ISHII'S CRIMES GIVING RISE TO FORFEITURE**

11 **Sony Life's plan to repatriate funds, following a corporate acquisition, to Japan**

12 27. Sony Life was a joint venture that partially owned Aegon Sony Life Insurance
13 Co. Ltd ("Aegon") and SA Reinsurance Ltd. ("SA Reinsurance"). In or about 2020, Sony
14 Life completed the acquisition of both Aegon and SA Reinsurance from the prior joint
15 venturer, Aegon NV.

16 28. After Sony Life completed those corporate acquisitions, its subsidiary
17 SA Reinsurance held funds in various accounts. Sony Life sought to repatriate those funds
18 to one or more bank accounts in Japan and it sought to do so through multiple transactions
19 that followed a similar pattern. First, Sony Life would transfer funds held in Japanese Yen
20 at international bank accounts to a Bermuda-based Citibank account. Second, the Japanese
21 Yen in the Bermuda-based Citibank account would, at times, be exchanged for U.S.
22 Dollars. Third, Sony Life would cause funds to be transferred from its Bermuda-based
23 Citibank account to an account in the name of Sony Life or one of its subsidiaries and held
24 at Sumimoto Mitsui Banking Corporation in Japan.

25 **Sony Life's setup of double-authentication funds-transfer process**

26 29. To execute these international funds transfers in a secure manner, Sony Life
27 initiated requests to transfer funds through Citibank's Secure Financial Transfer
28 Portal/Protocol ("SFTP"). SFTP is a messaging system with instructions for funds

1 transfers. Transfers initiated through SFTP require approvals from authorized users, or
2 Citibank clients. The Sony Life transactions described herein required double
3 authentication through email accounts of two Sony Life employees, Ishii and his
4 supervisor, K.Y.

5 30. On about July 29, 2020, Sony Life employee Ishii emailed to Citibank PDF
6 copies of notarized identification documents for K.Y. The purpose of sending these
7 documents was to establish K.Y.'s authority within the SFTP authentication process.

8 31. On December 15, 2020, Ishii sent Citibank an email requesting the original
9 email account attributed to K.Y. be changed from [K.Y.]@sonylife.co.jp² to [K.Y.]
10 @sareinsurance.com for purposes of accessing the SFTP system. The first of these email
11 addresses was K.Y.'s legitimate Sony Life email address but the second email address was
12 not a legitimate work email address for K.Y. as neither Sony Life nor its subsidiary SA
13 Reinsurance maintain any email account with the @sareinsurance.com domain name.

14 32. The request to change K.Y.'s email address initially was not honored by
15 Citibank because the action appeared suspicious. Ishii then contacted the Citibank help
16 desk to further his attempt to change K.Y.'s email address. In response to Ishii's contacts,
17 on or about February 17, 2021, Citibank finalized a change of K.Y.'s email address—from
18 K.Y.'s legitimate @sonylife.co.jp address to the @sareinsurance.com address—for
19 purposes of the SFTP authentication process.

20 **Ishii's April 22, 2021 international transfer of Sony Life funds with fraudulent**
21 **authorization but without converting the funds**

22 33. On April 22, 2021, Ishii initiated a transfer of Sony Life funds through the
23 SFTP authentication process, without proper authorization but also without converting any
24 Sony Life funds.

25 34. More specifically, on April 22, 2021, Ishii caused 41,781,771,935 Japanese
26 Yen to be transferred to a Bermuda-based Citibank account (#xxxx0272) and then

27 _____
28 ² The bracketed portion of this email address included the first and last name of Ishii's
supervisor K.Y.

1 transferred to Sony Life's account held at Sumitomo Mitsui Banking Corporation
2 (#xxxx6115).

3 35. Ishii caused the instructions for this transfer to be sent via SFTP and
4 authenticated by both Ishii's legitimate sonylife.co.jp address and the false
5 [K.Y.]@sareinsurance.com address that Ishii had fraudulently established in the name of
6 his supervisor K.Y.

7 36. The transfer was completed according to the instructions and Sony Life
8 received the transferred funds in its Sumitomo Mitsui account in Japan. Although Ishii
9 fraudulently used the false @sareinsurance.com email address to authenticate this
10 transaction, he did not convert any portion of the funds transferred on April 22, 2021, to
11 his own use.

12 **Ishii's May 18-20, 2021 international transfer of Sony Life funds Ishii had embezzled**
13 **and obtained by fraudulent authorization**

14 37. On or about May 18-20, 2021, Ishii fraudulently caused Citibank to initiate
15 another international fund transfer for Sony Life. He did so on the materially false
16 pretenses that he was conducting this transaction with Sony Life's approval and that he
17 was transferring the funds to an account controlled by an entity related to Sony Life. In
18 fact, he conducted this international fund transfer after he had taken steps to convert the
19 funds to his own use.

20 38. This time, Ishii initially caused Citibank to transfer 16,962,800,068 Japanese
21 Yen internationally to a Bermuda-based Citibank account (#xxxx9700). He then caused
22 Citibank to exchange the 16,962,800,068 Japanese Yen for 154,932,103.17 United States
23 Dollars. Although Ishii conducted these transfer and currency-exchange transactions in a
24 manner that appeared consistent with Sony Life's funds-transfer plan, Ishii had in fact
25 already obtained control of these funds by fraud. That is so because Ishii made the
26 international transfer of Sony Life funds on the false and fraudulent pretense that his
27 supervisor K.Y. had approved the transfer when, in fact, K.Y. had not done so.

28

1 39. Then, after fraudulently causing Citibank to make this transfer of Sony Life
2 funds to Bermuda, and causing Citibank to exchange 16,962,800,068 Japanese Yen for
3 154,932,103.17 United States Dollars, Ishii fraudulently wired instructions to Citibank,
4 through the same SFTP authentication process, to transfer the full \$154,932,103.17 amount
5 from the Sony Life account at Citibank in Bermuda to an account Ishii controlled at
6 Silvergate Bank. At least by that point, Ishii had converted these Sony Life funds, whose
7 control he had obtained by fraud, to his own use.

8 40. Specifically, as to the May 18-20, 2021 transactions, Ishii instructed Citibank
9 to transfer the full \$154,932,103.17 in Sony Life funds to a Coinbase credit account
10 (#xxxx0174) held at Silvergate Bank in La Jolla, California.

11 41. Ishii fraudulently authorized that transfer of \$154,932,103.17 in Sony Life
12 funds from Sony Life's Citibank account in Bermuda to the Silvergate Bank transaction
13 via the SFTP authentication process.

14 42. To complete that authorization process, Ishii used his legitimate sonylife.co.jp
15 address and fraudulently used the false [K.Y.]@sareinsurance.com address purportedly
16 belonging to Ishii's supervisor, K.Y.

17 43. In accordance with these instructions, Citibank transferred the 154,932,093.17
18 in funds to the Silvergate Bank account Ishii controlled. Ishii thus caused these funds,
19 which exceeded \$5,000 and which he knew he had obtained by fraud and had converted to
20 his own use, to be transmitted in foreign commerce from Bermuda to the United States.

21 44. According to Ishii's instructions, the funds transferred to Silvergate Bank
22 funded a Coinbase account (#xxxxf4da), which Ishii controlled.

23 45. As described below, Ishii had opened that Coinbase account associated with
24 the Silvergate Bank account on the materially false and fraudulent representations, which
25 involved use of interstate and international wires, that the account belonged to Sony Life's
26 subsidiary, SA Reinsurance, and that Ishii's supervisor, K.Y., was the individual associated
27 with the Coinbase account.

28

1 46. Ishii then caused the \$154,932,093.17 in funds transferred to his Silvergate
2 Bank and Coinbase account to be exchanged for approximately 3,879.16 bitcoin.

3 47. Ishii then caused Coinbase to transfer the approximately 3,879.16 bitcoin
4 from the Coinbase account Ishii controlled to a secure and encrypted “cold wallet,”
5 bc1q7rhc02dvhtmlfu8smywr9mayhdph85jlpf6paqu, which belonged to Ishii.

6 48. Ishii transferred the Sony Life funds he had stolen and obtained by fraud to
7 the Coinbase account that he held in a false name, and he then had Silvergate Bank and
8 Coinbase transfer that Bitcoin to a cold storage wallet. When Ishii made those transfers,
9 he knew that they were designed to conceal the nature, location, source, ownership, and
10 control of those proceeds of his fraud and embezzlement crimes.

11 49. Sony Life did not authorize the transfer of \$154,932,103.17 of its funds from
12 Citibank to Silvergate Bank and then to Coinbase.

13 50. Sony Life did not authorize Ishii to convert those Sony Life funds to Ishii’s
14 use.

15 **Ishii’s fraudulent opening of Coinbase account in name of Sony Life subsidiary**

16 51. On or about March 30, 2021, Ishii caused Coinbase to open account
17 #xxxxf4da. This was the cryptocurrency account that received proceeds from the
18 fraudulent transfer.

19 52. Ishii established this Coinbase account in the name of Sony Life’s subsidiary,
20 SA Reinsurance, and listed Ishii’s supervisor K.Y. as the individual associated with the
21 account.

22 53. Among the credentials that Ishii sent to Coinbase for account authentication
23 were PDF copies of notarized identification documents for K.Y., along with incorporation
24 documents for SA Reinsurance.

25 54. Ishii used these same or similar PDF documents to establish a fake email
26 account, supposedly belonging to Ishii’s supervisor K.Y., to provide K.Y.’s supposed
27 authority to transfer funds within Citibank’s SFTP authentication process.

28

1 55. When he opened this Coinbase account, Ishii had the account's unique user-
2 authentication PIN sent to his phone number +xx-xxx-xxx-4865. This phone number,
3 based in Japan, belongs to Rei Ishii. Ishii described this phone number as his personal
4 number in employment information that Ishii gave to the Sony Life's human resources
5 department. Ishii also listed this phone number in connection with travel records for trips
6 he took to the United States.

7 56. On April 1, 2021, Ishii established a rule for his Coinbase account that would
8 apply to any funds deposited into the account. The rule had the effect of transferring all
9 funds deposited into the account into a "cold wallet."

10 57. Ishii undertook the aforesaid actions knowing such a transfer was designed,
11 in whole or in part, of concealing the nature, source, location, ownership, and control of
12 funds that he later intended to steal from Sony Life.

13 **Ishii's ransom emails**

14 58. On May 25, 2021, Ishii anonymously sent an email to his supervisor K.Y.'s
15 official account at Sony Life. Ishii's message stated: "If you accept the settlement, we will
16 return the funds back." This message was transmitted and typed in English and Japanese.

17 59. The following day, on May 26, 2021, Ishii anonymously sent to K.Y. and
18 Sony Life executive T.H. an email at their official accounts stating: "If you are going to
19 file criminal charges, it will be impossible to recover the funds." "We might go down
20 behind all of this, but one thing is for sure, you are going to be right there next to us." This
21 message was also transmitted and typed in English and Japanese.

22 60. On May 27, 2021, Ishii anonymously sent to K.Y., T.H., and additional Sony
23 Life executives Ta.H., H.A., and H.K. an email at their official accounts stating: "If you
24 accept the settlement, we will return the funds back." "If you are going to file criminal
25 charges, it will be impossible to recover the funds." "We might go down behind all of this,
26 but one thing is for sure, you are going to be right there next to us." "We strongly
27 recommend to stop communicate (sic) with any third parties including law enforcement."
28

1 **VIII. NEXUS OF DEFENDANT 3879.16242937 BTC TO ISHII'S CRIMES**

2 61. Defendant is 3879.16242937 BTC that the Federal Bureau of Investigation
3 seized from a cold storage wallet belonging to Ray Ishi on or about December 1, 2021,
4 pursuant to a seizure warrant signed by the Honorable Mitchell D. Dembin, United States
5 Magistrate Judge for the Southern District of California, in Matter # 21MJ2528.

6 62. The Defendant 3879.16242937 BTC is traceable entirely to the
7 \$154,932,103.17 in money that Ray Ishii had stolen, converted, and taken by fraud from
8 Sony Life, via a scheme that involved material misrepresentations and international
9 wirings, including wirings to Silvergate Bank in the Southern District of California, all in
10 violation of Title 18, United States Code, Section 1343 (wire fraud).

11 63. The Defendant 3879.16242937 BTC is also traceable entirely to the
12 \$154,932,103.17 in money that Ray Ishii had stolen, converted, and taken by fraud from
13 Sony Life and caused to be transmitted and transferred in foreign commerce from Bermuda
14 to the United States and, specifically, to the Southern District of California, all in violation
15 of Title 18, United States Code, Section 2314.

16 64. The Defendant 3879.16242937 BTC was also involved in two concealment
17 money laundering transactions that Ishii committed in violation of Title 18, United States
18 Code, Section 1956. Specifically, on or about May 19-20, 2021, Ishii caused Silvergate
19 Bank, Coinbase, or both to exchange the \$154,932,093.17 in proceeds of Ishii's specified
20 unlawful activity, namely, wire fraud and international transfer of funds obtained by theft
21 and fraud, into bitcoin and to then further transfer that bitcoin to a cold storage wallet that
22 Ishii controlled. Those transactions were financial transactions because they involved the
23 use of financial institutions that were engaged in, and whose activities affected, interstate
24 and foreign commerce. When Ishii caused those financial transactions to be conducted, he
25 knew that the funds and BTC involved in those transactions were proceeds of unlawful
26 activities—his own. Ishii also conducted those transactions, using a Coinbase account at
27 Silvergate Bank that Ishii had opened in a nominee name, knowing full well that
28 those transactions were designed in whole or in part to conceal or disguise the nature, the

1 location, the source, the ownership, or the control of the proceeds of specified unlawful
2 activity. The Defendant BTC was therefore involved in two concealment money
3 laundering transactions that Ishii caused to be committed in violation of Title 18, United
4 States Code, Section 1956(a)(1)(B)(i).

5 65. The Defendant 3879.16242937 BTC was also involved in at least one
6 unlawful monetary transaction that Ishii committed in violation of Title 18, United States
7 Code, Section 1957. Specifically, on or about May 19, 2021, Ishii knowingly caused
8 Silvergate Bank and Coinbase, both financial institutions, to engage in a monetary
9 transaction, namely, exchanging the \$154,932,093.17 in funds into bitcoin. When Ishii
10 caused that monetary transaction to be conducted, he knew that the funds involved in that
11 transaction were derived from crime—crimes that he himself had committed. The
12 criminally derived funds involved in that transaction had a value of greater than \$10,000
13 and were also proceeds of Ishii's specified unlawful activity, namely, wire fraud and
14 international transfer of funds obtained by theft and fraud. The Defendant BTC was
15 therefore involved in an unlawful money laundering transaction that Ishii caused to be
16 committed in violation of Title 18, United States Code, Section 1957.

17 **IX. CLAIM FOR RELIEF**

18 66. The United States incorporates by reference the allegations in paragraphs one
19 (1) through sixty-five (65) above as though fully set forth herein.

20 67. The Defendant, Approximately 3879.16242937 bitcoin, seized from Bitcoin
21 address bclq7rhc02dvhtmlfu8smywr9mayhdph85jlpf6paqu, is property that constitutes or
22 was derived from proceeds traceable to violations of Title 18, United States Code, Sections
23 1343 (wire fraud) and 2314 (transferring or transmitting in foreign commerce money that
24 was stolen or taken by fraud) and is therefore subject to forfeiture to the United States in
25 accordance with Title 18, United States Code, Section 981(a)(1)(C), including cross
26 references to Title 18, United States Code, Sections 1956(c)(7)(A) and 1961(1)(B).

27 68. The Defendant BTC is also subject to forfeiture under Title 18, United States
28 Code, Section 981(a)(1)(A) as property involved in one or more transactions in violation

