IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
v.	:	**DATE FILED**
JUSTIN DAVID MAY	:	**VIOLATIONS:**
	:	**18 U.S.C. §§ 1341, 3559(g) (mail fraud – 24 counts)**
	:	**18 U.S.C. § 1956(a)(1)(B)(i) (money laundering – 16 counts)**
	:	**18 U.S.C. §§ 2314, 3559(g) (interstate transportation of goods obtained by fraud – 3 counts)**
	:	**26 U.S.C. § 7201 (tax evasion – 2 counts)**
	:	**18 U.S.C. § 2 (aiding and abetting)**
	:	**Notice of Forfeiture**

INDICTMENT

COUNTS ONE THROUGH FIFTEEN

THE GRAND JURY CHARGES THAT:

At all times relevant to this indictment:

1. Cisco is a corporation based in San Jose, California specializing in providing internet networking hardware and software for business, government, and individuals. Cisco's core development areas are in switching and routing, which enable Cisco customers to communicate through the use of the World Wide Web.

2. Cisco manufactures, sells, and supports computer networking equipment on a global scale. Cisco supports its products through two means: (a) a Limited Lifetime Hardware Warranty Program and Enhanced Limited Lifetime Warranty Program offered with

Cisco hardware and software (hereinafter a "Cisco Warranty"); and (b) a more comprehensive suite of support offered to customers for a fee (called and referred to by Cisco as "SMARTnet" Service).

3. The Cisco Warranty and SMARTnet Service are not transferrable. That means that any purchase of used or secondary-market Cisco equipment is not covered by the Cisco Warranty or SMARTnet Service even if it is purchased through a Cisco channel partner or distributor. Before used or secondary-market equipment can be placed under a new support contract, the requester must show proof of a valid software license or pay relicensing fees and must have the equipment inspected to confirm that it is in proper working order and has been maintained appropriately.

4. When a customer needs technical assistance on a device that is under Warranty or SMARTnet service, the customer can open a Cisco service request ("SR") and report its problem to Cisco in one of the following ways: by telephone, email, or through Cisco's website (www.cisco.com).

5. Cisco maintains Technical Assistance Centers ("TAC") worldwide to process these requests for service. All requests for service generate an SR number, which is used to track the reported problem until it is resolved. Upon creation of the SR, information about the customer is captured as well as the specific product complaint. Once initiated, the SR is sent to a Cisco TAC engineer for problem diagnosis and resolution. In some cases, based on the information provided by the customer, the resolution may require the replacement of the product in question. The TAC engineer will determine if the customer is entitled to a replacement product under the terms of Cisco's Limited Warranty Program or SMARTnet service.

6. If the customer is entitled to a replacement product, TAC will generate a Return Material Authorization ("RMA") reference number, initiating the process to deliver a replacement product to the customer. Under Cisco's Warranty and SMARTnet Service Programs, customers may be entitled to advance replacement, meaning that Cisco or one of its service centers will ship a replacement product to the customer before the customer sends back the faulty part, with the understanding that the faulty part will subsequently be returned to Cisco upon receipt by the customer of the replacement part. Cisco notifies customers who receive advance replacement that they must return the defective product.

7. Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin are not issued by any government, bank, or company, but rather are generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or pin needed to access the address. Only the holder of an address' private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses.

8. To transfer bitcoin to another address, the payor transmits a transaction announcement, cryptographically signed with the payor's private key, across the peer-to-peer Bitcoin network. The Bitcoin address of the receiving party and the sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a Bitcoin transaction itself. Once the

payor's transaction announcement is verified, the transaction is added to the blockchain, a decentralized public ledger that records all Bitcoin transactions. The blockchain logs every Bitcoin address that has ever received a bitcoin and maintains records of every transaction for each Bitcoin address.

9. To acquire Bitcoin, a typical user will purchase them from a Bitcoin "exchanger." Bitcoin exchangers generally accept payments of fiat currency (currency that derives its value from government regulation or law), or other convertible virtual currencies. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible virtual currency to an exchanger, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, usually for a commission, will then either sell the user bitcoin from the exchange's reserves or will attempt to broker the purchase with another user who is trying to sell bitcoin. The purchased bitcoin are then transferred to the purchaser's Bitcoin address, allowing the user to conduct transactions with other Bitcoin users via the Internet.

10. Virtual currencies, including Bitcoin, have known legitimate uses. However, given the ease with which Bitcoin can be used to move funds with high levels of anonymity, Bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds.

11. Boothwyn Check Cashing was a business located in Boothwyn, Pennsylvania, that provided check cashing, money order, bill payment, and money transmittal services.

12. Boothwyn Check Cashing customers could present checks to be cashed and receive in return the cash value of the check, minus Boothwyn Check Cashing's service charge.

13. In order to cash a check, Boothwyn Check Cashing customers were required to provide their name and address, present a valid form of identification each time they visited, and submit to having their photograph taken.

14. Softnetworks LLC was a business located in New Jersey that was in the business of reselling new and refurbished networking equipment, computers, and computer server products.

15. Computechsale LLC was a business located in New Jersey that was in the business of reselling new and refurbished networking equipment and computer-related products.

16. Defendant JUSTIN DAVID MAY had a checking account at Woodforest National Bank in ending in 2604.

THE SCHEME

17. Beginning in or about April 2016 and continuing until in or about April 2017, within the Eastern District of Pennsylvania and elsewhere, defendant

JUSTIN DAVID MAY

alone and with co-schemers known to the grand jury, devised and intended to devise a scheme to defraud and to obtain money and property by means of false and fraudulent pretenses, representations, and promises.

MANNER AND MEANS

18. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury obtained and ascertained serial numbers for Cisco computer hardware that defendant MAY did not own or possess.

19. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury verified with Cisco that the serial numbers he had obtained and ascertained were valid Cisco serial numbers for Cisco computer hardware.

20. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury registered false domain names.

21. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury took steps to prevent the effective identification of defendant MAY and the co-schemers as the persons who registered the false domain names and to effectively prevented Cisco and law enforcement from contacting defendant MAY and the co-schemers and tracking defendant MAY and the co-schemers by tracing the registration of the false domain names, including paying for the domain name registration with Bitcoin and utilizing a service called "WhoisGuard," which provided a level of anonymity for the person registering the domain name.

22. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury established email addresses using the false domain names that were design to mislead Cisco into believing that the email address was associated with a person who worked for a legitimate company.

23. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury used the false domain names and the email addresses he created tied to those false domain names to create false cisco.com user IDs.

24. Defendant JUSTIN DAVID MAY used the false domain name and e-mail addressed he created tied to those domain names, the false cisco.com user IDs he created, and the legitimate serial numbers that he had obtained and ascertained for Cisco computer hardware to submit approximately 266 false Cisco Warranty and Cisco SMARTnet service requests for Cisco

products that defendant MAY did not own or possess, which led to the creation of 266 SR numbers, all in an attempt to obtain by fraud computer hardware from Cisco with a retail value of approximately $4,044,260.

25. Co-schemers known to the grand jury used the false domain name and e-mail addresses they had created tied to those domain names, the false cisco.com user IDs they had created, and the legitimate serial numbers that they had obtained and ascertained for Cisco computer hardware to submit additional false Cisco Warranty and Cisco SMARTNET service requests in addition to the approximately 266 false Cisco Warranty and Cisco SMARTnet service requests for Cisco products that defendant JUSTIN DAVID MAY had submitted, which led to the creation of additional SR numbers in addition to the approximately 266 SR numbers defendant MAY had caused to be created, all in an attempt to obtain by fraud computer hardware from Cisco in additional to the approximately $4,044,260 in Cisco computer hardware defendant MAY had attempted to obtain.

26. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury communicated with Cisco TAC engineers by phone, email, and through online internet chat sessions posing as legitimate Cisco customers with faulty Cisco computer hardware that was covered by Cisco Warranty and Cisco SMARTnet coverage in order to induce Cisco to ship "replacement" computer hardware via Federal Express ("FedEx") for the supposedly faulty computer hardware that defendant MAY and his co-schemers claimed to own and possess.

27. Defendant JUSTIN DAVID MAY and co-schemers known to the grand jury provided Cisco TAC engineers with descriptions of the supposed problems with the computer hardware that defendant MAY and his co-schemers knew would prevent the TAC

engineers from solving the supposed problems through troubleshooting and would necessarily require the replacement of the supposedly faulty computer hardware.

28. Defendant JUSTIN DAVID MAY and his co-schemers represented to Cisco that they would return the supposedly faulty computer hardware to Cisco.

29. Defendant JUSTIN DAVID MAY, by his misrepresentations, successfully induced Cisco to ship approximately 169 pieces of valuable Cisco computer hardware to defendant MAY via FedEx, with a retail value of approximately $2,344,860.

30. Co-schemers known to the grand jury, by their misrepresentations, successfully induced Cisco to ship additional pieces of valuable Cisco computer hardware to the co-schemers via FedEx.

31. Defendant JUSTIN DAVID MAY provided Cisco with addresses at which Cisco could ship the computer hardware, including addresses in the Eastern District of Pennsylvania.

32. Defendant JUSTIN DAVID MAY tracked the shipment of the Cisco computer hardware through FedEx.

33. Defendant JUSTIN DAVID MAY contacted FedEx and changed the shipping address of shipments to FedEx stores in the Eastern District of Pennsylvania and elsewhere.

34. Defendant JUSTIN DAVID MAY traveled from his residence in the District of Delaware to the locations to which Cisco had shipped the computer hardware, including FedEx stores in the Eastern District of Pennsylvania, the District of Nevada, the District of Maryland, the District of New Jersey, and elsewhere.

35. Defendant JUSTIN DAVID MAY obtained the Cisco computer hardware from the locations to which it had been shipped, including from FedEx stores in the Eastern District of Pennsylvania, the District of Nevada, the District of Maryland, and the District of New Jersey, and elsewhere, by posing as the intended recipient.

36. Defendant JUSTIN DAVID MAY travelled with the fraudulent-obtained Cisco computer hardware across state lines, including from the Eastern District of Pennsylvania to his residence in the District of Delaware.

37. Defendant JUSTIN DAVID MAY ignored Cisco's repeated communications seeking the return of the supposedly faulty computer hardware, and did not return any computer hardware to Cisco, because defendant MAY had never owned the supposedly faulty computer hardware in the first place.

38. Defendant JUSTIN DAVID MAY sold the Cisco computer hardware he obtained in this manner to companies that were in the business of purchasing and reselling computer hardware, such as Computechsale LLC and Softnetworks LLC, both of which were located in New Jersey.

39. Defendant JUSTIN DAVID MAY travelled with the fraudulent-obtained Cisco computer hardware across state lines, including from his residence in the District of Delaware to Computechsale LLC and Softnetworks LLC in the District of New Jersey.

40. Defendant JUSTIN DAVID MAY received checks from Computechsale LLC and Softnetworks LLC for his sale of fraudulently-obtained Cisco computer hardware.

41. Defendant JUSTIN DAVID MAY converted checks he received for the sale of Cisco "replacement" computer hardware to cash by, among other things, cashing the checks at a check cashing company in the Eastern District of Pennsylvania.

42. Defendant JUSTIN DAVID MAY deposited some of the cash he received from the sale of the fraudulently-obtained Cisco computer hardware into his bank account ending in 2604 at Woodforest National Bank.

43. JUSTIN DAVID MAY used some of the proceeds from his sale of the fraudulently-obtained Cisco computer hardware to purchase a 2017 BMW coupe for approximately $62,246.

44. Defendant JUSTIN DAVID MAY used the 2017 BMW coupe to further his fraud scheme by driving it from the District of Delaware to the Eastern District of Pennsylvania, and elsewhere, to pick up additional "replacement" computer hardware that he obtained from Cisco by fraud as part of the fraud scheme.

45. Defendant JUSTIN DAVID MAY, by his actions as set forth herein, caused Cisco to ship computer hardware in response to approximately 169 of the approximately 266 separate fraudulent SRs submitted by defendant MAY. Of these approximately 169 shipments, defendant MAY successfully obtained from the delivery address approximately 155 pieces of valuable Cisco computer hardware, with a combined retail value of approximately $2,194,915, most of which defendant MAY subsequently sold.

MAIL FRAUD

46. On or about each of the following dates, in the Eastern District of Pennsylvania, the District of Nevada, and elsewhere, defendant

JUSTIN DAVID MAY

alone and with one or more co-schemers known to the grand jury, for the purpose of executing the scheme described above, and attempting to do so, and aiding and abetting its execution,

knowingly caused to be delivered by mail and commercial interstate carriers, according to the directions thereon, the following items:

COUNT	DATE	FROM	TO	DESCRIPTION OF ITEM
ONE	May 17, 2016	Roanoke, Texas	Jenkintown, Pennsylvania	Cisco Model # WS-3850-48P-S, retail value approximately $13,000, shipped via FedEx, tracking # 676893389930, in response to Cisco SR # 680370670
TWO	July 12, 2016	Roanoke, Texas	Springfield, Pennsylvania	Cisco Model # WS-C3850-48F-S, retail value approximately $14,000, shipped via FedEx, tracking # 690844892752, in response to Cisco SR # 680605046
THREE	July 20, 2016	Roanoke, Texas	Exton, Pennsylvania	Cisco Model # WS-C3850-48P-E, retail value approximately $21,000, shipped via FedEx, tracking # 690844956492, in response to Cisco SR # 680640480
FOUR	July 20, 2016	Roanoke, Texas	Wayne, Pennsylvania	Cisco Model # WS-C3850-48T-S, retail value approximately $11,500, shipped via FedEx, tracking # 690844956301, in response to Cisco SR # 680640796
FIVE	July 25, 2016	Roanoke, Texas	Wynnewood, Pennsylvania	Cisco Model # WS-3850-48PW-S, retail value approximately $14,500, shipped via FedEx, tracking # 690844993122, in response to Cisco SR # 680662587
SIX	August 18, 2016	Roanoke, Texas	Philadelphia, Pennsylvania	Cisco Model # WS-3850-48P-L, retail value approximately $10,400, shipped via FedEx, tracking # 701630826669, in response to Cisco SR # 680796102

COUNT	DATE	FROM	TO	DESCRIPTION OF ITEM
SEVEN	November 28, 2016	Roanoke, Texas	Malvern, Pennsylvania	Cisco Model # ASR-9001, retail value approximately $53,600, shipped via FedEx, tracking # 714903325940, in response to Cisco SR # 681366926
EIGHT	December 13, 2016	Roanoke, Texas	King of Prussia, Pennsylvania	Cisco Model # ASR-9001, retail value approximately $53,600, shipped via FedEx, tracking # 714903461631, in response to Cisco SR # 681449650
NINE	March 9, 2017	Roanoke, Texas	Springfield, Pennsylvania	Cisco Model # WS-C3850-48P-S, retail value approximately $13,000, shipped via FedEx, tracking # 725509138044, in response to Cisco SR # 681939335
TEN	March 13, 2017	Roanoke, Texas	Plymouth Meeting, Pennsylvania	Cisco Model # WS-C3850-48T-S, retail value approximately $11,500, shipped via FedEx, tracking # 725509156499, in response to Cisco SR # 681957029
ELEVEN	March 15, 2017	Roanoke, Texas	Philadelphia, Pennsylvania	Cisco Model # WS-C3850-48P-L, retail value approximately $11,500, shipped via FedEx, tracking # 725509179950, in response to Cisco SR # 681975518
TWELVE	March 30, 2017	Roanoke, Texas	Reno, Nevada	Cisco Model # WS-C3850-48U-S, retail value approximately $14,500, shipped via FedEx, tracking # 725509278820, in response to Cisco SR # 682067937
THIRTEEN	March 30, 2017	Roanoke, Texas	Reno, Nevada	Cisco Model # WS-C3850-48U-S, retail value approximately $14,000, shipped via FedEx, tracking # 725509279919, in response to Cisco SR #682068285

COUNT	DATE	FROM	TO	DESCRIPTION OF ITEM
FOURTEEN	April 3, 2017	Roanoke, Texas	Philadelphia, PA	Cisco Model # WS-C3850-48U-L, retail value approximately $11,400, shipped via FedEx, tracking # 729853483641, in response to Cisco SR # 682084775
FIFTEEN	April 3, 2017	Roanoke, Texas	Philadelphia, PA	Cisco Model # WS-C3850-48U-L, retail value approximately $11,400, shipped via FedEx, tracking # 729853482976, in response to Cisco SR # 682085341

All in violation of Title 18, United States Code, Sections 1341, 3559(g), and 2.

COUNTS SIXTEEN THROUGH TWENTY-FOUR

THE GRAND JURY FURTHER CHARGES THAT:

1. Paragraphs 7 through 10 of Count One are incorporated here.

At all times relevant to this indictment:

2. Microsoft is a corporation based in Redmond, Washington that produces computer software and hardware, including the Microsoft Surface, a personal computer that can function as a laptop or tablet.

3. Microsoft manufactures, sells and supports its hardware on a global scale. The Microsoft Surface comes standard with a one-year warranty. Customers can purchase additional warranties through a handful of Microsoft approved distributors. When warranties and associated devices are purchased, the distributor sends Microsoft a record of the Surface device serial numbers and the associated warranty. Microsoft tracks this information and if a customer wants to confirm their device serial number and verify their warranty status, they can use an internet browser and navigate to https://mybusinessservice.surface.com.

4. Microsoft Enterprise customers are businesses or public sector customers who meet user and device volume thresholds set by Microsoft. Enterprise customers are afforded numerous benefits, including volume pricing discounts, a dedicated customer service channel and enhanced warranty options. Under certain circumstances, Enterprise customers with a qualifying warranty may opt for an "Advanced Exchange" of their device.

5. Advanced Exchange is a warranty replacement program where, in certain circumstances, customers are immediately shipped a replacement device with the agreement that they will return their problematic device to Microsoft as stipulated in the Microsoft Device Service Order Terms and Conditions. In order to initiate an Advanced Exchange, a customer

must be eligible based on their specific device, issue, and warranty status as determined by the serial number of their device.

6. To initiate an Advanced Exchange, the customer calls the Microsoft Global Customer Service Center to speak with a customer service agent who will address their issue. The customer service agent will first assess the customer's complaint about their Surface device. If the Surface device is inoperable or needs repair, the customer service agent will recommend an exchange. Customers contacting customer service with a defective or damaged device who have a valid Microsoft Complete warranty for that device will be given an opportunity to use the Advanced Exchange service.

THE SCHEME

7. Beginning in or about August 2017 and continuing until in or about November 2017, within the Eastern District of Pennsylvania and elsewhere, defendant

JUSTIN DAVID MAY

alone and with one or more co-schemers unknown to the grand jury, devised and intended to devise a scheme to defraud and to obtain money and property by means of false and fraudulent pretenses, representations, and promises.

MANNER AND MEANS

8. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury obtained and ascertained serial numbers for Microsoft Surface devices that defendant MAY did not own or possess.

9. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury registered false domain names.

10. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury took steps to prevent the effective identification of defendant MAY and the unknown co-schemers as the persons who registered the false domain names and to effectively prevented Microsoft and law enforcement from contacting defendant MAY and the co-schemers and tracking defendant MAY and the co-schemers by tracing the registration of the false domain names, including paying for the domain name registration with Bitcoin and utilizing a service called "WhoisGuard," which provided a level of anonymity for the person registering the domain name.

11. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury established email addresses using the false domain names that were design to mislead Microsoft into believing that the email address was associated with a person who worked for a legitimate business.

12. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury used the false domain names, e-mail addressed they created tied to those false domain names, and legitimate serial numbers that they had obtained and ascertained for Microsoft Surface devices to submit approximately 227 false Microsoft Advanced Exchange warranty claims for Microsoft products that defendant MAY and his co-schemers did not own or possess, all in an attempt to obtain by fraud computer hardware from Microsoft with a retail value of over $600,000.

13. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury communicated with Microsoft Customer Service Representatives by phone, email, and through online internet chat sessions posing as legitimate Microsoft Surface device customers with faulty Microsoft computer hardware that was under warranty and eligible for the

Microsoft Advanced Exchange program in order to induce Microsoft to ship "replacement" computer hardware via United Parcel Service ("UPS") and Federal Express ("FedEx") for the supposedly faulty computer hardware that defendant MAY and his co-schemers claimed to own and possess.

14. Defendant JUSTIN DAVID MAY and more or more co-schemers unknown to the grand jury provided Microsoft Customer Service Representatives with photographs that purported to be true and correct photographs of legitimate serial numbers of Microsoft Surface devices but were in fact false and altered photographs.

15. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury provided Microsoft Customer Service Representatives with descriptions of the supposed problems with the computer hardware that defendant MAY and his co-schemers knew would prevent the Microsoft Customer Service Representatives from solving the supposed problems through troubleshooting and would necessarily require the replacement of the supposedly faulty computer hardware.

16. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury represented to Microsoft that they would return the supposedly faulty computer hardware to Microsoft.

17. Defendant JUSTIN DAVID MAY and one or more co-schemers unknown to the grand jury provided Microsoft with addresses at which Microsoft could ship the computer hardware, including addresses in the Eastern District of Pennsylvania.

18. Defendant JUSTIN DAVID MAY and his co-schemers, by their misrepresentations, induced Microsoft to ship approximately 139 Surface devices, with a retail value of approximately $393,000 to defendant MAY and his co-conspirators via UPS and FedEx