

PASCO COUNTY COMPLAINT AFFIDAVIT

PSO FLO 510000 NPR PD FLO 510200 PR PD FLO 510400
DC PD FLO 510100 ZPD FLO 510300 FHP FLO 279000

OBTS NUMBER 5102131909 FELONY MISD. CO. ORD. CIVIL INF. SHIFT 1 SECTOR 05 SEC 12 TWP. 12 RING. 12 AGENCY REPORT NUMBER 18-27651
ARREST CHECK ALL THAT APPLY 1. FELONY 2. TRAFFIC FELONY 3. MISD. 4. MISD. TRAFFIC 5. ORDINANCE 6. OTHER 7. V.O.P. 8. PROBABLE CAUSE 9. CIVIL INF. ADULT JUVENILE

NOTICE TO APPEAR CHECK ONLY ONE MANDATORY APPEARANCE NON-MANDATORY APPEARANCE JUVENILE NON / ARREST REF. REQUEST FOR CHECK ONLY ONE CAPIAS WARRANT SUMMONS JUV. PICK-UP REVIEWED BY ASSISTANT STATE ATTORNEY DATE
LOCATION OF ARREST (INCLUDE NAME OF BUSINESS) 9733 Lake Chrise Ln. Port Richey, FL, 34668 LOCATION OF OFFENSE (BUSINESS NAME, ADDRESS) Same

DATE OF ARREST 07/18/2018 TIME OF ARREST 0915 BOOKING TIME 7/18/18 1148 JAIL DATE 7/18/18 JAIL TIME 1148 WEAPON SEIZED YES NO WEAPON TYPE F.P.S.S. Notified Y N Juv. Elderly Handicap
JAIL NUMBER 210564 FDLE NUMBER 02883607 DOC NUMBER FBI NUMBER Domestic Related Y N

NAME (LAST, FIRST, MIDDLE) ALIAS HANDSCHUMACHER, Ricky CONVICTED SEXUAL PREDATOR/OFFENDER Y N
RACE W WHITE H HISPANIC I AMERICAN INDIAN O ORIENTAL / ASIAN CODE W SEX M DATE OF BIRTH 03/31/1993 AGE 25 HEIGHT 601 WEIGHT 230 EYE COLOR Blue HAIR COLOR Red COMPLEXION Fair BUILD Med
SCARS, MARKS, TATTOOS, ETC. INDICATION OF: ALCOHOL INFLUENCE DRUG INFLUENCE

PHYSICAL ADDRESS (STREET & APT #) (CITY) (STATE) ZIP PHONE RESIDENCE TYPE 1. CITY 2. COUNTY 3. FLORIDA 4. OUT OF STATE CODE 2
MAILING ADDRESS (STREET & APT #) (CITY) (STATE) ZIP PHONE ADDRESS SOURCE Defendant
BUSINESS ADDRESS (NAME & STREET) (CITY) (STATE) ZIP PHONE OCCUPATION City Worker

DRIVER'S LICENSE STATE / NUMBER H532730931110 SOCIAL SECURITY NUMBER INS NUMBER PLACE OF BIRTH NY CITY OF BIRTH FLORIDA

CO-DEFENDANT NAME (LAST, FIRST, MIDDLE) RACE SEX DATE OF BIRTH AGE 1. ARRESTED 2. AT LARGE 3. FELONY 4. MISDEMEANOR 5. JUVENILE
CO-DEFENDANT NAME (LAST, FIRST, MIDDLE) RACE SEX DATE OF BIRTH AGE 1. ARRESTED 2. AT LARGE 3. FELONY 4. MISDEMEANOR 5. JUVENILE

NAME OF PARENT OR CUSTODIAN (LAST, FIRST, MIDDLE) PARENT LEGAL CUSTODIAN OTHER
ADDRESS (STREET, APT NUMBER) BUSINESS PHONE

NOTIFIED BY (NAME) DATE TIME JUVENILE DISPOSITION 1. HANDLED / PROCESSED WITHIN DEPT. AND RELEASED 2. TURNED OVER TO HRS / CYF 3. INCARCERATED COUNTY
RELEASED TO (NAME) RELATIONSHIP DATE TIME

CHARGE DESCRIPTION Money Laundering > \$100,000.00 F.S. CIVIL INF. STATUTE VIOLATION NUMBER 896.101(3)(a)2a NCIC # COURT CASE # 18CF004271AWS.2
ACTIVITY S. SELL R. SMUGGLE K. DISPENSE/DISTRIBUTE M. MANUFACTURE PRODUCE / CULTIVATE Z. OTHER CODE N AMOUNT 0 TYPE N. N/A B. BARBITURATE H. HALLUCINOGEN P. PARAPHERNALIA / EQUIPMENT U. UNKNOWN Z. OTHER CODE N
N. N/A B. BUY D. DELIVER E. USE T. TRAFFIC

CHARGE DESCRIPTION Grand Theft > \$100,000.00 F.S. CIVIL INF. STATUTE VIOLATION NUMBER 812.014(2)(a) NCIC # COURT CASE # 18CF004271AWS.1
ACTIVITY S. SELL R. SMUGGLE K. DISPENSE/DISTRIBUTE M. MANUFACTURE PRODUCE / CULTIVATE Z. OTHER CODE N AMOUNT 0 TYPE N. N/A B. BARBITURATE H. HALLUCINOGEN P. PARAPHERNALIA / EQUIPMENT U. UNKNOWN Z. OTHER CODE N
N. N/A B. BUY D. DELIVER E. USE T. TRAFFIC

REQUEST FOR INVESTIGATIVE COSTS RECOVERY FSS 938.27(1) THE UNDERSIGNED CERTIFIES AND SWEARS THAT HE / SHE HAS JUST AND REASONABLE GROUNDS TO BELIEVE, AND DOES BELIEVE THAT THE ABOVE-NAMED DEFENDANT COMMITTED THE FOLLOWING VIOLATION OF LAW:
CJIS # 3513 ON THE 18th DAY OF July, 2018 AT 0800 A.M. P.M.
of Investigative hrs. 36 x 26.00 = \$936.00 \$0.00

(SPECIFICALLY INCLUDE FACTS CONSTITUTING CAUSE FOR ARREST.)
Please see attached affidavit

P.C. EXISTS FOR CHARGE(S) JUDGE'S SIGNATURE DATE
I AGREE TO APPEAR AT THE TIME AND PLACE DESIGNATED WHEN I AM NOTIFIED TO ANSWER THE OFFENSE CHARGED OR TO PAY THE FINE SUBSCRIBED. I UNDERSTAND THAT SHOULD I WILLFULLY FAIL TO APPEAR BEFORE THE COURT AS REQUIRED ONCE I AM NOTIFIED, THAT I MAY BE HELD IN CONTEMPT OF COURT AND A WARRANT FOR MY ARREST SHALL BE ISSUED. IF CITED FOR A CIVIL INFRACTION, I AGREE TO APPEAR BEFORE THE COUNTY COURT OR COMPLY WITH THE REQUIREMENTS FOR PAYING THE FINE AND MEETING ANY OTHER SPECIFIED CONDITIONS AS INDICATED ON THE BACK SIDE OF THIS AFFIDAVIT.

SIGNATURE OF DEFENDANT / JUVENILE AND PARENT OR CUSTODIAN DATE
MIRANDA WARNING HOLD FOR OTHER AGENCY VERIFIED BY RIGHT THUMB DATE VICTIM NOTIFIED YES NO BOND CHARGE # \$50,000 \$50,000

ADULT ONLY HOLD FOR FIRST APPEARANCE DO NOT BOND OUT - REASON: UNDER PENALTIES OF PERJURY, I DECLARE THAT I HAVE READ THE FOREGOING (DOCUMENT) AND THAT THE FACTS STATED IN IT ARE TRUE TO THE BEST OF MY KNOWLEDGE AND BELIEF.
X Det. D. Stewart 3513 NAME (PRINTED) CJIS #
BOND / COURT INFO. BOND TYPE 1. ROR 2. CASH 3. SURETY 4. BAIL / BOND 5. CERT 6. OTHER TYPE RETURNABLE COURT DATE RETURNABLE COURT TIME A.M. P.M.
RELEASE DATE RELEASE TIME A.M. P.M.
RELEASING OFFICER PAGE PAGE 1 OF 2


DEFENDANT						AGENCY REPORT NO. 18-27651							
CHARGE DESCRIPTION Offenses Against Computers to Facilitate Fraud						<input checked="" type="checkbox"/> F.S. <input type="checkbox"/> ORD.	STATUTE VIOLATION NUMBER 815.06(3)(b)2			NCIC #	COURT CASE # 13CFO04271AWS.3		
ACTIVITY N. N/A P. POSSESS	S. SELL B. BUY T. TRAFFIC	R. SMUGGLE D. DELIVER E. USE	K. DISPENSE / DISTRIBUTE	M. MANUFACTURE PRODUCE / CULTIVATE	Z. OTHER	CODE	AMOUNT	TYPE N. N/A A. AMPHETAMINE	B. BARBITURATE C. COCAINE E. HEROIN	H. HALLUCINOGEN M. MARIJUANA O. OPIUM / DERV	P. PARAPHERNALIA / EQUIPMENT S. SYNTHETIC	U. UNKNOWN Z. OTHER	CODE
CHARGE DESCRIPTION						<input type="checkbox"/> F.S. <input type="checkbox"/> ORD.	STATUTE VIOLATION NUMBER			NCIC #	COURT CASE #		
ACTIVITY N. N/A P. POSSESS	S. SELL B. BUY T. TRAFFIC	R. SMUGGLE D. DELIVER E. USE	K. DISPENSE / DISTRIBUTE	M. MANUFACTURE PRODUCE / CULTIVATE	Z. OTHER	CODE	AMOUNT	TYPE N. N/A A. AMPHETAMINE	B. BARBITURATE C. COCAINE E. HEROIN	H. HALLUCINOGEN M. MARIJUANA O. OPIUM / DERV	P. PARAPHERNALIA / EQUIPMENT S. SYNTHETIC	U. UNKNOWN Z. OTHER	CODE

N/A

CMT 3 - \$10,000

UNOFFICIAL DOCUMENT

NARRATIVE / CONTINUATION

ADMINISTRATIVE	UNDER PENALTIES OF PERJURY, I DECLARE THAT I HAVE READ THE FOREGOING (DOCUMENT) AND THAT THE FACTS STATED IN IT ARE TRUE, TO THE BEST OF MY KNOWLEDGE AND BELIEF.	
	X 	
	D. STEWART	3513
	NAME (PRINTED)	CJIS #

CLERK OF COURT

PROBABLE CAUSE

AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT DS

I, Daniel Stewart, after being duly sworn, depose and state as follows:

I. INTRODUCTION AND DETECTIVE BACKGROUND

1. Your Affiant is a duly sworn law enforcement officer employed by the Pasco Sheriff's Office (PSO) since October, 2009 and was so employed during all times stated herein. During the past eight (8) years, Your Affiant has served the PSO as a Deputy Sheriff in the Uniform Patrol Division, the Criminal Investigations Bureau, and the Special Investigations Division.
2. From 2013 – 2016 Your Affiant was assigned in the PSO Economic Crimes Unit. During this time, Your Affiant investigated numerous Economic Crime complaints to include credit card fraud, worthless documents (checks), identity theft, counterfeit currency and exploitation of the elderly cases.
3. Your Affiant is currently assigned to the Special Investigations Division of the PSO and has been assigned to this unit since 2016. Your Affiant's responsibilities inside this unit include working money laundering, wire fraud, bank fraud, human trafficking and other cases associated with finances and narcotics.
4. Your Affiant is currently on the Homeland Security Investigations (financial group) task force. As a member of the task force, Your Affiant has the authority to investigate crimes of the United States Criminal Code pertaining to, among other things, bank fraud, wire fraud, and money laundering.

5. Your Affiant has received over 80 hours of training on asset forfeiture and money laundering and has attended classes regarding International Money Laundering, Bulk Cash Smuggling, and Terrorist Financing.
6. Your Affiant has investigated and arrested individuals for RICO and Money Laundering offenses against Florida State Statutes.
7. Information contained in this affidavit is based on information personally known to me, told to me by other law enforcement officers, or based upon my previous investigative experiences.
8. This affidavit does not cover all knowledge of the case, only the information relevant to establish probable cause. The information contained in this affidavit is obtained from valid sources, resources, reports and interviews.
9. As a Deputy Sheriff, Your Affiant is authorized to investigate violations of the laws of the Florida State Statutes and execute arrest and search warrants issued under the authority of the State of Florida.

A. COMMON METHODS USED BY MONEY LAUNDERS

10. Through my training and experience, one of the most difficult steps in the money laundering process is introducing the illicit funds into the financial system. Money launders do this in numerous ways.
11. Another process in the laundering phase is known as layering. In this phase, the money launderer conducts a series of transactions, transfers, or purchases to disguise, conceal or discombobulate the true source of funds. Often in this process, money launders will exchange currency denominations (small bills for

large bills) and/or types (United States Currency for Euro's, cryptocurrencies, etc...).

II. APPLICATION FOR WARRANT TO ARREST

12. Your Affiant submits this affidavit for the purpose of obtaining an arrest warrant for Ricky HANDSCHUMACHER. Your Affiant began investigating Ricky HANDSCHUMACHER (herein after referred to as HANDSCHUMACHER) after receiving information from Homeland Security Investigations (herein after referred to as HSI) in Detroit. HSI is a federal law enforcement agency.

B. DEFINITION(S)

13. Florida State Statute § 896.101 defines "Conducts" as initiating, concluding, or participating in initiating or concluding a transaction.

14. Florida State Statute § 896.101 defines "Transaction" as a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safety deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected.

15. Florida state Statute § 896.101 defines "Financial institution" as a financial institution as defined in 31 U.S.C. s. 5312 which institution is located in this state.

- 16.31 U.S.C s 5312 defines a financial institution as a currency exchange (section J), a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system (section R).
17. Florida State Statute § 896.101 defines “Financial transaction” as a transaction involving the movement of funds by wire or other means or involving one or more monetary instruments, which in any way or degree affects commerce, or a transaction involving the transfer of title to any real property, vehicle, vessel, or aircraft, or a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, commerce in any way or degree.
18. Florida State Statute § 896.101 defines “Knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity” as the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under state or federal law...
19. Florida State Statute § 896.101 defines “Monetary instruments” as coin or currency of the United States or of any other country, virtual currency, travelers’ checks, personal checks, bank checks, money orders, investment securities in bearer form or otherwise in such form that title thereto passes upon delivery, and negotiable instruments in bearer form or otherwise in such form that title thereto passes upon delivery.

20. Florida State Statute § 815.03 defines a computer as an internally programmed, automatic device that performs data processing.
21. Florida State Statute § 896.101 defines “Specified unlawful activity” as racketeering activity defined in 895.02.
22. Florida State Statute § 895.02(8) defines “Racketeering activity” as committing, to attempt to commit, to conspire to commit, or to solicit, coerce, or intimidate another person to commit:
- (32) Chapter 812, relating to theft, robbery, and related crimes.
 - (33) Chapter 815, relating to computer-related crimes.
23. Merriam-Webster defines Cryptocurrency as “any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions”
24. Merriam-Webster defines Bitcoin as “a digital currency created for use in peer-to-peer online transactions”
25. Merriam-Webster defines Blockchain as “a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network; also : the technology used to create such a database”
26. Merriam-Webster defines SIM Card as “a card that is inserted into a device (such as a cell phone) and that is used to identify a subscriber on a communications network and to store data (such as phone numbers or contact information)”

27. A TREZOR is defined as “a single purpose device which allows you to make secure Bitcoin transactions. With TREZOR, transactions are completely safe even when initiated on a compromised or vulnerable computer.”
28. Gemini is an online cryptocurrency exchange that buys and sells cryptocurrencies for United States Currency.
29. Coinbase is an online cryptocurrency exchange that buys and sells cryptocurrencies for United States Currency.
30. Bittrex is an online cryptocurrency exchange that buys and sells cryptocurrencies for United States Currency.
31. Monero is a type of cryptocurrency.
32. Xmr is a cryptocurrency wallet.

C. APPLICABLE STATUTE VIOLATIONS

a. Money Laundering

33. Florida State Statute § 896.101 is known as the Florida Money Laundering Act.

34. Florida State Statute § 896.101(3) states: It is unlawful for a person:

(a) Knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or attempt to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity:

1. With the intent to promote the carrying on of specified unlawful activity; or
2. Knowing that the transaction is designed in whole or in part:

- a. To conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
- b. To avoid a transaction reporting requirement or money transmitters' registration requirement under state law.

b. Grand Theft

35. Florida State Statute § 812.014(1) states: A person commits theft if he or she knowingly obtains or uses, or endeavors to obtain or to use, the property of another with intent to, either temporarily or permanently:

(a) Deprive the other person of a right to the property or a benefit from the property.

(b) Appropriate the property to his or her own use or to the use of any person not entitled to the use of the property.

36. Florida State Statute § 812.014(2)(a) states: If the property stolen is valued at \$100,000 or more... the offender commits grand theft in the first degree, punishable as a felony of the first degree, as provided in s. 775.082, s. 775.083, or s. 775.084.

c. Offenses Against Users of Computers

37. Florida State Statute § 815.06(2) states: A person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization:

- a. Accesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized;
- b. Disrupts or denies or causes the denial of the ability to transmit data to or from an authorized user of a computer, computer system, computer network, or electronic device, which, in whole or in part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;

38. Florida State Statute § 815.06(3)(b)2 states: A person commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if he or she violates subsection (2) and: Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property;

III. PROBABLE CAUSE

A. The Background

i. Detroit, Michigan

i. The Investigation

39. On or around February, 2018 the Canton Police Department, located in Michigan, began investigating an individual after the individual's mother overheard him talking on the phone pretending to be an AT&T employee.

40. Officers responded to the scene and made contact with the individual (hereinafter referred to as CS1). Officers gained consent to search CS1's computer, person, and room. Officers discovered shortcuts labeled "ATT Plug" and TMobile Plug" on the computer. When Officers opened the shortcuts, it produced an extensive

list of names and phone numbers of people from around the world. Officers discovered multiple SIM cards on the desk and four (4) cell phones on CS1's person.

41. Officers located a messaging service on CS1's laptop, which revealed a conversation between CS1 and other individuals regarding ways to defraud AT&T.
42. On or around March 2018, Officers observed CS1 in a public library viewing personal identifying documents. Officers seized forty-five (45) SIM cards, a laptop, and a TREZOR device.
43. On or around April 2018, Officers responded to CS1's residence after CS1's mother called law enforcement to tell them he/she was in possession of another cell phone. Officers gained consent to search the room and discovered two bags of SIM Cards, and a cell phone. Officers conducted another forensic examination of the items and found numerous personal identification information such as driver's licenses and passports.
44. Officers identified seven (7) victims from the SIM cards found in CS1's possession. The victims included residents from New York, California, North Carolina, Vermont, Michigan, Texas, and Utah.
45. Officers contacted the victims and learned someone stole their identity along with large sums of money from various bank accounts.
 - c. Victim 1 told officers her cell phone was compromised and she lost control of her cell phone and e-mail account. After regaining

control, she learned \$50,000.00 was stolen from her Gemini account.

- d. Victim 2 told officers his cell phone and e-mail account were compromised and he was locked out of one account valued at \$150,000.00 and is unable to determine if the money was stolen.
- e. Victim 3 told officers his cell phone and cryptocurrency accounts were compromised and \$150,000.00 was stolen from his Gemini account. Victim 3 told officers the theft occurred on or around May 18, 2018.

46. Officers conducted surveillance on CS1 in May 2018. Officers observed CS1 receive a package from a residence and travel to a bank where he made a \$900.00 cash deposit.

47. Officers learned CS1 was receiving a package from Georgia. Officers obtained a search warrant for the package and learned it contained SIM cards and was addressed to CS1. Officers arrested CS1 and learned there was another package addressed to him/her. Officers discovered the second package contained approximately \$8,000.00 in United States Currency.

48. Officers executed a search warrant at CS1's residence and discovered additional electronic equipment, government identification cards, and mailing packages. HSI agents seized approximately \$200,000.00 in stolen cryptocurrency from CS1.

ii. The Interview

49. CS1 spoke to law enforcement officers. Post Miranda, CS1 told officers he/she purchased cryptocurrency usernames through the internet. CS1 along with a group of individuals, to include HANDSCHUMACHER, obtained SIM cards in order to clone the phone of victims.
50. Once the phones were cloned, the group would gain access to the victim's e-mail accounts and cryptocurrency exchanges to include Gemini and Coinbase. Once the group gained access to the account, they would use the victim's funds to purchase cryptocurrencies and transfer it to an accounts the group controlled. After CS1 received the funds, he would store them on the TREZOR device law enforcement officers previously seized. CS1 admitted to purchasing items online and to exchanging the cryptocurrency for cash using an online website where the money would be sent to him/her.
51. CS1 said he/she would communicate with approximately eight (8) individuals in order to commit the fraud scheme. One of the individuals CS1 identified was Ricky HANDSCHUMACHER. The individuals used an online chat databases such as Discord and Telegram to communicate with each other.
52. CS1 said he would chat with the coconspirators on a daily basis to obtain victim identities and attempt to hack their financial accounts. CS1 said the group has been conducting the fraud since December 2016. CS1 told officers HANDSCHUMACHER used the handle @coinmission in their chat. Officers learned HANCSCUMACHER resides in Pasco County, Florida and contacted

HSI-Tampa for further investigation. HSI requested the assistance of the Pasco Sheriff's Office in the case.

B. The Lead

i. Pasco County, Florida

53. HSI Detroit provided your affiant with evidence they obtained from search warrants, forensic examinations, and consent searches. Your affiant observed a chat conversation that occurred on May 16, 2018. The chat took place between 12:50 hours and 19:23 hours. In the conversation, the username @goldenspeed typed the name "Ricky" and asked a question. The username @coinmission responded to the question. In the conversation, HANDSCHUMACHER, using the name @coinmission, explained he purchased land, a house, a vehicle, and a quad vehicle.

54. The conversation identifies a phone number and a SIM number. The group worked together to steal 57 Bitcoins from the victim. According to an open source website, the price of Bitcoin that day was \$8,240.27 per coin. This means the group stole \$469,695.39. Later in the conversation, a co-conspirator claims they stole \$513,000.00 and agreed to split it between them for a total of \$128,000.00 each.

C. The Laundering

55. In the same conversation, the group discussed a way to launder the money by using different cryptocurrency exchanges and cryptocurrencies. The conversation states "bitcoin > shapeshift to monero > send monero to xmr.to and get clean b tc back."

56. This conversation tells the group to use a cryptocurrency exchange to sell the cryptocurrency they stole to purchase another cryptocurrency called Monero. After they acquired the Monero currency, they would send it to another cryptocurrency wallet called "xmr." After the cryptocurrency was in the xmr wallet, they would exchange the Monero for Bitcoin. Because of the multiple wallets, and the sale and purchase of cryptocurrencies, this makes the new purchased Bitcoin appear to come from a legitimate source.
57. Your affiant believes the transactions occurred this way to launder and conceal the true source of funds.

D. Search Warrant and Subpoena Results

58. Your Affiant viewed the search warrant and subpoena results provided by law enforcement officers in Detroit. Your affiant observed subpoena results from an online cryptocurrency exchange called Coinbase.
59. Coinbase provided HANDSCHUMACHER's name, driver's license number, date of birth, address, debit card number, phone number, cryptocurrency wallet identifiers, and IP addresses. The address provided by Coinbase listed HANDSCHUMACHER's address. Coinbase also provided law enforcement officers with a picture of HANDSCHUMACHER's Florida driver's license which lists HANDSCHUMACHER's address. Law enforcement officers conducted an analysis on the account and determined there was a total of 82.67013567 BTC sold or sent from this account, of which 81.72072 BTC was received from outside sources.

60. In the subpoena results, Coinbase identifies IP address 68.200.110.179 associated with accessing HANDSCHUMACHAER's account approximately 99 times between May 10th, 2017 and April 30th, 2018.
61. Your affiant observed a Discord conversation obtained through a search warrant. The warrant results identify HANDSCHUMACHER's username as "lolsmileyface." In the information, HANDSCHUMACHER states his other chat username is Coinmission. The results show the account was accessed using IP address 68.200.11.179 approximately 274 times between April 18, 2018 and June 15, 2018. Coinbase provided this same IP address to officers. In the conversation, HANDSCHUMACHER claims he has six (6) figures worth of cryptocurrency.
62. Later in the same conversation, HANDSCHUMACHER and another co-conspirator talk about compromising the CEO of Gemini and posted his name, date of birth, Skype username and e-mail address in the conversation. HANDSCHUMACHER and the co-conspirator discuss compromising the CEO's Skype account and T-Mobile account. The co-conspirator states he will call his "guy" at T-Mobile to ask about the CEO's account.
63. HANDSCHUMACHER and the co-conspirator continue to discuss exchanging different cryptocurrencies to get their portion of the fraud. They even discuss the cryptocurrencies being "dirty" and discuss laundering over \$100,000.00 in cryptocurrencies.
64. Records provided by Coinbase show the buying, selling, and trading of cryptocurrencies in ways that would appear consistent with CS1's statements.

65. HANDSCHUMACHER confessed post Miranda that he laundered in excess of \$100,000.00 in cryptocurrency within the past year. HANDSCHUMACHER also stated he used his cellular phone to facilitate the cryptocurrency transfers.

IV. Summary

Since December 2016, Ricky HANDSCHUMACHER along with other co-conspirators conspired together to commit multiple grand thefts from victims throughout the United States.

HANDSCHUMACHER along with the co-conspirators would identify victims and acquire their personal identification information without permission of the individual. Once the information was obtained, they would either pay an individual at a cellular service company or call and represent themselves as an employee of a cellular service company and have a new SIM card activated with the victim's information.

Once the group obtained control of the phone, they would compromise the victim's e-mail accounts and cryptocurrency wallets and steal the victim's funds by transferring the cryptocurrency into wallets controlled by members of the group.

Once the funds were in wallets controlled by the group, the victims' funds were split and distributed into the fraudsters individual wallets. The group would launder the funds by using online cryptocurrency exchanges to exchange one cryptocurrency (ie: Bitcoin) to another (ie: Monero). After the currency was converted, it would be transferred into another wallet owned by the individual and resold to another cryptocurrency. That cryptocurrency would be sent to the final destination wallet controlled by the fraudster using another cryptocurrency

exchange. By this time, the currency simply appears as a legitimate transaction from the sale of the previous cryptocurrency and is successfully laundered.

Records obtained from law enforcement officers and statements made by cooperating individuals identify screen names belonging to Ricky HANDSCHUMACHER. In the conversations, co-conspirators mention HANDSCHUMACHER by his first name and HANDSCHUMACHER answers the question, acknowledging he is the individual conducting the communication and transactions. In the conversation, HANDSCHUMACHER made a reference to having six figures worth of cryptocurrency in his possession. Records provided by Coinbase, a cryptocurrency exchange, identify Ricky using a picture of his Florida driver's license, his name, date of birth, and address. Records from Coinbase show Ricky's wallet was accessed using the same IP address used on one of the chat conversations where the group committed a theft and admitted to stealing crypto currency.

HANDSCHUMACHER confessed to his involvement in the crime post Miranda and admitted to using his cell phone to launder cryptocurrency in amounts greater than \$100,000.00.

V. CONCLUSION

66. Based on the forgoing facts, Your Affiant submits that probable cause exists to arrest Ricky HANDSCHUMACHER.

67. Your Affiant respectfully requests this affidavit be sealed and exempt from public record.

FURTHER YOUR AFFIANT SAYETH NAUGHT.



Daniel J. Stewart

Pasco County Sheriff's Office

Vice / Narcotics Detective

UNOFFICIAL
DOCUMENT