

AO 91 (Rev. 11/11) Criminal Complaint

FILED

SEALED

UNITED STATES DISTRICT COURT

for the

Western District of Texas

FEB - 6 2018

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY [Signature]
DEPUTY

United States of America
v.

Case No. SA: 18-MJ-0148

Christina Thistlethwaite

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September 21, 2015 through July 11, 2017 in the county of Bexar and other counties in the Western District of Texas, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 USC §§1029(a)(2);	Fraud with more than one Access Device of over \$1,000.00 in one year period;
1029(a)(5); and	Fraud with more than one Access Device issued to another person of over \$1,000.00 in one year period; and
1028A(a)(1).	Aggravated Identity Theft.

This criminal complaint is based on these facts:

See Attached Affidavit

Continued on the attached sheet.

[Signature]
Complainant's signature

Parker Dippel, S/A - USSS

Printed name and title

- Sworn to before me and signed in my presence.
- Sworn to telephonically and signed electronically.

Date: 2/6/2018

[Signature]
Judge's signature

City and state: San Antonio, TX

RICHARD FARRER, United States Magistrate Judge

Printed name and title

<p>Max Penalties: 1029a 2--10 years imprisonment, 3 years S/R, 250,000 fine, 100 Special Assessment 1029a 5--15 years imprisonment, 3 years S/R, 250,000 fine, 100 Special Assessment 1028A(a)(1)--mandatory 2 years imprisonment, 250K fine, 1 year S/R, 100 Special Assessment</p>
--

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION**

Affidavit In Support Of Criminal Complaint And Arrest Warrant

1. I, Parker W. Dippel, being duly sworn do hereby depose and state that I am a Special Agent with the United States Secret Service (USSS) assigned to the San Antonio Field Office. I have been a Special Agent of the USSS since August, 2014. I have been a law enforcement officer for approximately ten years. As a Special Agent of the United States Secret Service, I received extensive training on conducting investigations on violations of Federal law at the Federal Law Enforcement Training Center and the Secret Service James J. Rowley Training Center. I am assigned to the Secret Service South Texas Regional Task Force (STRTF) with the objective to aggressively identify and investigate financial and electronic state and federal criminal violations in the Western District of Texas.
2. The following information and statements contained in this affidavit are based upon information obtained from the United States Air Force Office of Special Investigations(AFOSI) and other criminal investigative agencies and information your Affiant learned in the during this investigation, including information from financial institutions, witnesses, and others participating in the investigation. This affidavit does not purport to set forth all of my knowledge or investigation concerning this case.
3. I am presently investigating the activities of Christina Thistlethwaite whom I have probable cause to believe has violated Title 18 United States Code (USC), 1029 (a)(2), 1029(a)(5), and 1028A(a)(1).
4. Title 18 U.S.C. Section 1029(a)(2) (Access Device Fraud) prohibits knowingly and with intent to defraud, trafficking in or using one or more unauthorized access devices during any one year period, and by such conduct, obtains anything of value aggregating \$1,000.00 or more in that period. Title 18 U.S.C. Section 1029(a)(5) (Access Device Fraud) prohibits knowingly and with intent to defraud, effecting transactions with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1 year period, the aggregate value of which is equal to or greater than \$1,000.00. Title 18 USC Section 1028A(a)(1) (Aggravated Identity Theft) prohibits knowingly transferring, possessing, or using without lawful authority a means of

identification of another during and in relation to any felony enumerated in subsection (c). Access device fraud pursuant to 1029(a)(2) and 1029(a)(5) both qualify as an enumerated felony under the Aggravated Identity Theft statute.

5. Your affiant knows that SA Jarvis Beauchamp has been Air Force Office of Special Investigation (AFOSI) Special Agent since 2017 and that he received his training and certification at the Federal Law Enforcement Training Center. He has 11 years law enforcement experience. Since then, SA Beauchamp has been involved in the investigation of a variety of cases involving persons of military interest, including but not limited to child exploitation, fraud and sexual assault investigations. SA Beauchamp has received specialized training and certification in Economic Crimes Investigations and Analysis.
6. On June 20, 2017, based on information provided by Officer KENNETH JOHNSON, 502d Security Forces Squadron (SFS), Joint Base San Antonio (JBSA)-Fort Sam Houston (FSH), TX, that CHRISTINA THISTLETHWAITE (THISTLETHWAITE), 4414 Amandas Cove, San Antonio, TX, carried out a scheme to defraud using the identity of VICTIM 1, San Antonio, TX. Specifically, THISTLETHWAITE opened a Military Star Card credit card in VICTIM 1's name and established herself as an authorized purchaser on VICTIM 1's account. Afterward, THISTLETHWAITE made \$19,261.93 in fraudulent purchases at Base Exchanges at JBSA-Randolph, TX, JBSA-FSH, TX, and JBSA-Camp Bullis, TX within the Western District of Texas. All purchases were captured on Army & Air Force Exchange Service (AAFES) security camera footage and seized by 502 SFS as evidence. All JBSA Base Exchanges are exclusive federal jurisdiction. AFOSI assumed primary investigative responsibility. THISTLETHWAITE was a Licensed Vocational Nurse (LVN) who worked at various medical facilities as a contract LVN. Her targets were largely elderly patients to which she had access as part of LVN duties.
7. AFOSI reviewed records and surveillance footage, which revealed THISTLETHWAITE, applied for and opened a Military Star Card credit account associated to VICTIM 1 via AAFES' website. THISTLETHWAITE changed the billing address to her own and established herself as an authorized purchaser for the account. Between May 22 and June 6, 2017, THISTLETHWAITE went to multiple AAFES stores on military bases across JBSA within the Western District of Texas and conducted numerous fraudulent purchases totaling

\$19,261.93. These purchases included, but were not limited to, thirty one (31) Vanilla Visa Gift credit cards with a combined value of \$12,500, at a time when VICTIM 1 was in the hospital.

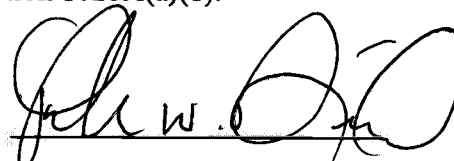
8. AFOSI reviewed records and surveillance footage which revealed on June 19, 2017, THISTLETHWAITE changed the billing address to her own address for a Military Star Card credit card account which belonged to VICTIM 2 from San Antonio, TX. On July 6, 2017, THISTLETHWAITE personally obtained a temporary credit card from the AAFES store in VICTIM 2's name. THISTLETHWAITE made numerous purchases at various JBSA-Fort Sam Houston AAFES stores, which totaled \$6,988.33. Purchases included, but were not limited to, sixteen (16) Vanilla Visa Gift credit cards with a combined value of \$7,350. VICTIM 2 was in the hospital at the time.
9. AFOSI reviewed a Vanilla Visa Gift credit card transaction report, which disclosed from July 6 through July 11, 2017; THISTLETHWAITE utilized the gift cards at numerous merchants in San Antonio, TX. On July 8, 2017, THISTLETHWAITE utilized the Vanilla Visa Gift card #3962 to make a \$40.00 payment to renew her own LVN license with the State of Texas. THISTLETHWAITE also purchased premium subscriptions to Truthfinder.com, White Pages Premium, and Docusearch.com.
10. Your affiant knows the credit cards used constitute unauthorized "access devices" because the pertinent legal definition of the term access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other means of account access that can be used, alone or in conjunction with another access device to obtain money, goods, services, or any other thing of value, or can be used to initiate a transfer of funds.
11. AFOSI reviewed Hays County Texas Sheriff's Office (HCSO) incident report, which disclosed an ongoing investigation into THISTLETHWAITE from September 21, 2015 through May 2, 2016. The HCSO determined THISTLETHWAITE accessed USAA account information for forty four (44) individuals, thirty three (33) of whom were hospital patients where THISTLETHWAITE worked at the time. During HCSO's interview, THISTLETHWAITE confessed to stealing patients' personal information and using websites to research if the individuals had good credit to determine if they were viable targets for exploitation. THISTLETHWAITE conducted fraudulent activity totaling \$49,500 during the

mentioned timeframe. Forensic examination of her cellular phone revealed the phone number associated to the device was the same phone number USAA Investigators captured when THISTLETHWAITE called to access the individual's accounts. Further, Internet Protocol addresses were identified which were matched to internet fraudulent purchases THISTLETHWAITE made with Best Buy. The evidence shows that Thistlethwaite knew she was using the means of identification of real persons.

12. AFOSI reviewed Hays County Sheriff's Office's (HCSO) report involving THISTLETHWAITE. During the HCSO's investigation the total amount of fraudulent activity discovered to be attributed to THISTLETHWAITE's fraudulent activity was \$49,500. These amounts were spread across two separate victims associated with this case: VICTIM 3 from San Marcos, TX (\$6,500 in fraudulent credit card charges) and a second VICTIM not clearly identified had a fraudulent \$43,000.00 USAA loan taken out in the victim's name. Det ANGELO FLORIAN, HSCO, contacted USAA who revealed THISTLETHWAITE contacted USAA using her own telephone number, which was captured by USAA. THISTLETHWAITE then accessed forty four (44) individuals' respective account information and changed those account addresses to Thistlethwaite's own address, which matched the address on THISTLETHWAITE's Texas Driver's License at the time. HSCO also determined THISTLETHWAITE used a different last name as an alias. While the last name was different, the social security number, driver's license, and phone number all resolved back to THISTLETHWAITE. SA BEAUCHAMP later met with USAA Financial Crimes Investigations. As of September 15, 2017 USAA estimated THISTLETHWAITE's fraudulent activity at approximately \$189,660.
13. On April 27, 2017, ANGELO along with other HSCO officers and San Antonio Police Department officers executed a search warrant at THISTLETHWAITE's former residence (4414 Amandas Cove, San Antonio, TX). During the search warrant ANGELO conducted an consensual interview of THISTLETHWAITE at the residence. THISTLETHWAITE verbally provided the following information: Initially, THISTLETHWAITE denied any involvement in fraudulent activity. ANGELO presented her with the information obtained from USAA's investigation which showed forty four (44) separate individuals' accounts had the address changed to THISTLETHWAITE's residence. Those address changes were telephoned in. The number USAA captured on each was THISTLETHWAITE's phone

number. ANGELO advised he discovered over the course of his investigation that thirty three (33) of the forty four (44) individuals were patients at the hospital. THISTLETHWAITE broke down, cried, and apologized profusely. THISTLETHWAITE, who worked at the hospital, confessed to taking patients' personal identifying information (PII) from the paper charts she had access to. THISTLETHWAITE then took the information and researched individuals' information at Lending Tree's website, where she obtained their credit reports. THISTLETHWAITE analyzed each target she identified to exploit to determine if they were a viable target with good credit. THISTLETHWAITE denied having any of the fraudulent credit cards in her possession. THISTLETHWAITE discarded them once she was unable to charge merchandise any longer. THISTLETHWAITE mentioned in addition to merchandise, she often bought gift cards and presented them as presents to her friends and family. THISTLETHWAITE related she committed the fraud in order to cover living expenses and because she fell behind on bills.

14. Your affiant knows that conducting transactions to receive merchandise with a credit card at various military bases and elsewhere within the Western District of Texas necessarily affects interstate commerce, both in the way the credit card infrastructure receives its electronic information over state lines as well as the way the military base engages in interstate commerce to provide goods and services for sale. The evidence shows Thistlethwaite affected interstate commerce when she conducted the fraudulent credit card transactions.
15. Your affiant believes that the foregoing facts show probable cause that Thistlethwaite committed felony violations of access device fraud in violation of Title 18 U.S.C. Section 1029 (a)(2), Section 1029(a)(5) and Section 1028A(a)(1).



Special Agent Parker Dippel
United States Secret Service

SUBSCRIBED AND SWORN TO BEFORE ME on February 6th, 2018.



RICHARD FARRER
UNITED STATES MAGISTRATE JUDGE