AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of Illinois

United States of America
v.
Josef V. Bita

Case No. 24-mj-6415

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 April 25, 2024 in the county of Rock Island in the Central District of Illinois, the defendant(s) violated:

Code Section	*Offense Description*
Title 18 United States Code 1029(a)(3)	Possession of 15 or More Counterfeit or Unauthorized Access Devices

This criminal complaint is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

s/Jeremy McAuliffe

Complainant's signature

Jeremy McAuliffe, USSS Task Force Officer

Printed name and title

Sworn to before me and signed ~~in my presence and/or~~ by reliable electronic means.

Date: April 26, 2024

s/Karen L McNaught

Judge's signature

City and state: Springfield, Illinois

Karen L. McNaught, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Jeremy McAuliffe, being duly sworn on oath, hereby depose and state:

1. I have been employed as a peace officer with the City of Moline, Illinois since 1996 and sworn as a Special Federal Officer and/or Task Force Officer with the United States Secret Service for over ten years. During my course of duties, I conduct investigations of violations of federal statutes involving the financial crimes, sexual exploitation of minors, cybercrime, and child pornography. I have completed numerous training courses related to electronic crimes and computer devices. During my career, I have regularly conducted investigations into access device fraud. As a Special Federal Officer and/or Task Force Officer, I am authorized to investigate violations of the United States Code relating to counterfeit and unauthorized access devices in violation of 18 USC §1029(a)(3), fraud and related activity in connection with access devices.

2. I make this affidavit in support of an application for criminal complaint and arrest warrant of JOSEF V BITA.

3. I submit that probable cause exists to believe that Bita violated 18 USC §1029(a)(3), knowingly and with intent to defraud possessing 15 or more counterfeit or unauthorized access devices.

4. The following is based on my personal investigation as well as receipt of information from other federal and local law enforcement personnel. I have not set forth all the information known to me or known to other members of law enforcement. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Bita has violated 18 USC §1029(a)(3).

BACKGROUND REGARDING ACCESS DEVICE FRAUD

5. Card encoders are commonly available on-line for about $100 and have valid commercial uses for, among many reasons, employee access control, inventory control, or time-keeping. The encoder is connected via a USB cable and specialized software is installed on the computer.

6. Generally, credit cards, debit cards, gift cards and even hotel room key cards all contain a magnetic strip on the back. That magnetic strip contains three tracks. For cards used for retail purchases, one track will contain the account number, the second the account holder name, and the third is not always used. In the case of gift cards, the account holder track would be empty as well. Occasionally, the third track could contain information related to a particular store's loyalty rewards program.

7. Re-encoding a card is a relatively simple affair. The desired account information is loaded into the software and, as a credit, debit, or gift card is passed through the encoder, the magnetic strip on the back of the card is reprogrammed with the new information.

8. Credit card and gift card account information can be easily obtained on the internet from "carding" sites where the information is sold for varying prices based on the quality of the information. Gift Card account numbers can also be simply guessed by a bad actor after observing the account numbers in a retail store.

9. Gift cards in a store have no inherent value until activated by someone purchasing the card and placing value in the card's account. An individual can take note of these account numbers prior to being sold at a store. After a period of time, they can call a phone number or check a retailer's website to check the residual value of the card. Once an individual has found a gift card with value loaded onto it, they will re-encode another gift card with the account

information. Retailers have become wise to this technique and implemented daily limits to the number of balance inquiries allowed from a particular phone number or computer.

10. Once re-encoded with the unauthorized account information, the card can be used as normal or sold for a fraction of the stored value on the account.

11. Card information can also be obtained via skimming devices placed on ATM machines, gas pumps, and other credit card reading devices. Skimming devices are inserted into the card reader and used to electronically read the data on the magnetic strip of the card and record the data. Debit cards also require a PIN and many skimming devices will also be installed with a camera on the ATM to record the PIN numbers.

PROBABLE CAUSE

12. On April 24, 2024, Moline Police department responded to IH Mississippi Valley Credit Union (IHMVCU), 2500 River Drive Moline, Illinois, and were advised a skimming device and camera had been installed and discovered on the ATM. Employees for IHMVCU advised they were checking all the ATMs as another skimmer had been placed on an ATM machine in East Moline, Illinois. Employees of IHMVCU reviewed the surveillance footage from the ATM and found at 1813 hours on April 24, 2024, a maroon Ford Windstar pulled up to the ATM with two subjects in the van. The driver, who was later identified as Bita, places something in the ATM. A minor male in the passenger seat, later identified as R.M., hands Bita a large flat object that Bita also places on the ATM. R.M. appears to be communicating with someone on the telephone as they are placing the objects. The two then leave. The large flat object was removed from the ATM and found to have a camera pointed at the key pad on the ATM. A skimmer was also removed from the card slot of the ATM. Employees for IHMVCU also advised a skimming device and camera were placed on this same ATM and then removed the following morning on

April 20, 2024, April 21, 2024, and April 22, 2024. The skimming device and camera were removed from the ATM and collected as evidence.

13. Employees for IHMVCU also advised another skimming device was located on the ATM at 2101 52nd Avenue Moline, Illinois. Employees for IHMVCU and officers then responded to this location and the skimmer and camera were removed and collected as evidence. The skimmer and camera set up were very similar in design to the ones identified in the paragraph above.

14. The East Moline Police Department also took a report from employees for IHMVCU on April 24, 2024 for a skimming device that had been placed on the ATM located at 358 17th Avenue East Moline, Illinois. Employees for IHMVCU reported that they had received an alarm for the ATM on April 23, 2024 at 1745 hours, but nothing was found. In reviewing video from the ATM, they watched two subjects in a blue Ford Focus hatchback placing and removing apparent skimming devices on April 22, 2024, April 23, 2024, and April 24, 2024. The devices were installed by the same two people in the blue Ford Focus hatchback after 1700 hours and removed early the next morning. Based on video surveillance a license plate of IL ER43346 was discovered for the blue Ford Focus Hatchback. I later identified the two subjects as Minors A.M and V.N. after viewing the still images from the ATM and speaking with the two subjects at the Moline Police Department.

15. On April 25, 2024, the Moline Police Department received reports from citizens that their IHMVCU account was accessed at ATMs in Moline and money withdrawn without their card being lost. Officers had been looking for the maroon Ford Windstar and Blue Ford Focus Hatchback. Officers located the Blue Ford Focus Hatchback in East Moline, Illinois in the 600 block Avenue of the Cities. The Blue Ford Focus Hatchback was parked next to the Gray

Pontiac Torrent in the parking lot for the UPS Store and Subway. Contact was made with the subjects. Minor R.M. was in the front passenger seat and Bita was standing in the open driver's door threshold the gray Pontiac Torrent, and Minors V.N. and A.M. were in the Blue ford Focus Hatchback. Minor V.N. was in the driver's seat of the Blue ford focus Hatchback.

16. Officers found Bita was sealing a cardboard box with tape as they made contact. Bita told officers he was in the US legally and lived in Baltimore, but was originally from Romania. Bita advised he was visiting unknown friends in Moline and when asked about the box he was sealing, he said he found it in the gray Pontiac Torrent and did not know what was in it. Bita also advised the gray Pontiac Torrent was one of the other three's car. Bita's wallet was found next to the gear box, along with two apparent fake identification cards (Ireland passport card and Canadian driver's license) with Bita's photographs, but with the name of Giovani Preotu and a different date of birth than Bita later gave police. Officers recognized Bita and minor R.M. from photos in a bulletin put out of the subjects placing the skimmer device on the ATM in Moline. Minors V.N and A.M. were recognized from photos obtained from IHMVCU and included in the East Moline Police Report as the subjects placing the skimming devices on the ATM in East Moline, Illinois. All four subjects were detained and brought to the Moline Police Department. Both vehicles were also towed to Quad City Towing. A black iPhone with cracked rear glass was seized from Minor A.M.'s person when he was transported to the police department.

17. Continuing on April 25, 2024, Detective Griffin obtained a State of Illinois search warrant for both vehicles. During the search of the Gray Pontiac Torrent, a black duffle bag was located in the rear seat behind the driver's seat. Inside the bag were various tools for cutting, gluing, and soldering items. There was also a gray Evolve laptop with S/N EBOOK1121013019584, skimmer templates and recording devices, USB cables with

connections for reading data for the skimming devices and pin hole cameras, and battery packs. Another black backpack was also found in the back seat. Inside the backpack was a stack of Vanilla Visa cards with stickers containing four digit numbers hand written on them, consistent with PIN numbers. There was also a MicroSD card inside the back compartment of the backpack. The cardboard box was found to have two pinhole camera devices and a blank template for a camera. Both camera devices appear to have a storage device attached to them. The Vanilla Visa cards were later run through a card reader and found to have different credit card numbers encoded on them than what appear printed on the face of the card. Several of the encoded account numbers were found to be from IHMVCU. There was also an iPhone in a Burberry case and a blue iPhone with cracked rear glass. The only evidence located in the blue Ford Focus Hatchback was a gray iPhone with cracked front and rear glass.

18. I spoke with Bita and provided him with his *Miranda* rights. Bita advised he is from Romania and is not legally here in the United States. Bita advised he crossed the border and was given a court date by border patrol, but did not go to his court date. Bita also acknowledge that he was arrested in Orlando, Florida a year ago for possessing fraudulent credit cards. Bita advised he possessed the fraudulent Ireland passport card and Canadian driver's license to get into clubs. Bita denied being involved in any skimming activity and said he stayed in the hotel or AirBnB while the others were out. Bita advised the four of them stayed together and that minor R.M. was related to him. Bita also identified his cell phone as the blue iPhone with cracked rear glass and was allowed to access the device to obtain phone numbers for family.

19. Minor R.M. was interviewed and would not talk about the skimming activity. Minor R.M. was shown an image of two subjects placing the skimming device on the ATM located at 2500 River Drive Moline, IL. Minor R.M. identified himself as the passenger and Bita as the

driver. I have also reviewed the still images from the Moline ATM at 2500 River Drive and believe the subjects also to be Bita and Minor R.M. Minor R.M. was able to use his cell phone, which he identified as the iPhone in the Burberry case to get contact information to try and contact his parents.

20. Minors A.M. and V.N. both requested attorneys and declined to give statements. Minor V.N. identified his phone as the gray iPhone with the cracked front and rear glass as his and was able to use it to get phone numbers to try and contact parents.

21. All of the seized cell phones and evidence was stored in temporary evidence at the Moline Police Department.

22. Bita and the three Minors were all arrested for charges related to credit card fraud. The Minors were detained by juvenile probation and Bita was transported to the Rock Island County Jail.

23. On April 26, 2024, Detective Cody Parmenter scanned all of the cards that were seized from the backpack, with the exception of one card that was broken in half and not scanned. There were a total of fifty cards. The other forty-nine cards were scanned and all confirmed to have different account numbers encoded on their magnetic strips than what appear printed on the face of the card. All of the encoded numbers have accounts belonging to IHMVCU based on the first six digits of the accounts.

CONCLUSION

24. Based on the foregoing, I assert there is probable cause to conclude Josef V. Bita has violated 18 USC §1029(a)(3).

Respectfully submitted,

s/Jeremy McAuliffe

Jeremy McAuliffe
Detective, Moline Police Department
Task Force Officer, U.S. Secret Service

s/Karen L McNaught

KAREN L. McNAUGHT
UNITED STATES MAGISTRATE JUDGE