

**AFFIDAVIT OF SPECIAL AGENT [REDACTED] IN SUPPORT OF  
A CRIMINAL COMPLAINT AND ARREST WARRANTS**

I, [REDACTED], state:

***INTRODUCTION AND AGENT BACKGROUND***

1. I am a Special Agent with Homeland Security Investigations (HSI) assigned to the Providence Field Office. I have been employed by HSI and its predecessor, the U.S. Customs Service since January of 2003. In connection with my official duties, I have investigated and assisted other agents in investigating numerous cases involving a wide variety of criminal violations including, but not limited to, narcotics trafficking, money laundering, interstate transportation of stolen property bank fraud, wire fraud and access device fraud.

2. The information contained in this affidavit is based on witness interviews, conversations with investigators from multiple agencies/ departments involved in this investigation, my personal knowledge and observations during the course of this investigation, my personal training and experience as a criminal investigator, and the review of records, documents and other evidence obtained during this investigation. Because this affidavit is submitted for the limited purpose of establishing probable cause for the requested arrest warrants, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to support the warrants requested herein.

3. I am currently investigating several known and unknown individuals

(hereinafter referred to as the “Target Subjects”) for violations of various federal statutes, including 18 U.S.C. § 1029(b)(2), (conspiracy to commit access device fraud), 18 U.S.C. §§ 1344 and 1349, (conspiracy to commit bank fraud), and 18 U.S.C. § 1028A(a)(1) and (c)(5), (aggravated identity theft), (collectively, the “Target Offenses”).

#### ***PURPOSE OF AFFIDAVIT***

4. I submit this affidavit in support of an application for a criminal complaint and arrest warrants for the following six individuals:

- Nicolas Longin CODREANU, age 21, is a citizen of Romania and Ireland who last entered the United States on or about October 10, 2017, and has since overstayed the conditions of his admission;<sup>1</sup>



- Ionut ZAMFIR, age 36, is a citizen of Romania who last entered the United States illegally on or about May 5, 2022;

---

<sup>1</sup> Nicolas Longin CODREANU entered the United States under the Visa Waiver Program (VWP). The VWP allows citizens of certain participant countries, including Ireland, to enter the United States without a visa and remain for a period of up to 90 days.



- Armando Ion CODREANU, age 23, is a citizen of Ireland who last entered the United States illegally at an unknown place and time;<sup>2</sup>



- Isabela Ignat CODREANU, age 23, is a citizen of Romania who last entered the United States illegally on or about May 6, 2021;

---

<sup>2</sup> Armando Ion CODREANU last attempted to legally enter the United States on May 16, 2017, under the VWP. However, U.S. Customs and Border Protection (CBP) Officers determined that he was inadmissible at that time. Based on the circumstances on his inspection, CBP Officers believed that Armando Ion CODREANU was coming to the United States to illegally work and remain longer than the conditions of his entry would allow.



- Mila CIUCIU, a/k/a Mila CIUCIUC, age 20, is a citizen of Romania who last entered the United States on or about November 12, 2016;



- Robby Vicson CODREANU, age 20, is a citizen of Great Britian who last entered the United States illegally at an unknown place and time;



(Hereinafter, the “Target Subjects”) as described further in Attachment A.

5. Collectively, the Target Subjects have multiple arrests in various states. The following is a list of known law enforcement contacts with the Target Subjects:

- Nicolas Longin CODREANU – Nicolas Longin CODREANU was arrested in February of 2020 in Cypress, CA, for receiving stolen property. During the time of this arrest, CODREANU also provided a fraudulent identity document. In December of 2020, CODREANU was arrested in Anaheim, CA for burglary and fraudulent use of a scanning device, while he was tampering with several ATM machines. Following this arrest, CODREANU also provided a fraudulent identity document to law enforcement. In March of 2024, CODREANU was convicted of four different state statutes stemming from this December 2020 incident and received 2 years’ probation. In April of 2022, CODREANU was arrested for driving without a license and providing a false identification to law enforcement. CODREANU was convicted of these two offenses in March of 2024 and sentenced to pay a fine and one day in jail. In November of 2023, CODREANU was arrested in Los Angeles County, CA for burglary and possession of burglary tools.

- Ionut ZAMFIR – Ionut ZAMFIR was arrested in May of 2022, by the U.S. Border Patrol in Texas after he illegally crossed into the United States from Mexico.
- Armando Ion CODREANU – Armando Ion CODREANU was arrested in April of 2024, in Knoxville, TN for identity theft and attempted theft while in possession of ATM skimming equipment and burglary tools.
- Isabela Ignat CODREANU – Isabela Ignat CODREANU was first arrested in February of 2018 in Washington by U.S. Border Patrol after illegally crossing in the United States from Canada. Isabela Ignat CODREANU was arrested again in May of 2021 by the U.S. Border Patrol in California after illegally crossing into the United States from Mexico.
- Mila CIUCIU – Mila CIUCIU was arrested in December of 2022 by Pennsylvania State Police for retail theft.<sup>3</sup>
- Robby Vicson CODREANU – Robby Vicson CODREANU was arrested in April of 2024, in Knoxville, TN for identity theft and attempted theft while in possession of ATM skimming equipment and burglary tools.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that the Nicolas Longin CODREANU, Ionut ZAMFIR, Armando Ion CODREANU, Isabela Ignat CODREANU, Mila CIUCIU, and Robby Vicson CODREANU conspired to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2), while Nicolas Longin CODREANU, Ionut ZAMFIR, and Armando Ion CODREANU also engaged in a conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 1344 and 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) and (c)(5),

---

<sup>3</sup> Mila CIUCIU was also encountered by U.S. Border Patrol in 2010 and again in 2016 as a juvenile, while attempting to enter the United States with her family.

(collectively, the “Target Offenses”).

### **SKIMMING/ACCESS DEVICE SCHEMES**

7. I know based upon my training and experience, conversations with other law enforcement officers, and review of similar cases involving skimming devices that Automated Teller Machines (ATMs) are electronic devices operated by financial institutions for use by banking customers to conduct banking transactions, such as withdrawing money from accounts. ATMs are often located on the premises of financial institutions and other business establishments.

8. A standard ATM requires the user to identify themselves as a particular banking customer by inserting a unique credit or debit card with a magnetic strip that stores data about the user’s bank account into a card reader. The ATM then requires the cardholder to verify his or her identity by typing a unique personal identification number (PIN) onto a provided keypad. Once the correct PIN is entered by the user, the ATM provides the user access to the user’s bank account, which can include permitting the user to withdraw a specific amount of available funds from the account in the form of currency. In this way, credit and debit cards and PINs used at ATMs function as “access devices,” as that term is defined in 18 U.S.C. § 1029(e)(1).

9. Many ATMs are connected to interbank networks, which communicate over interstate wires and enable a banking customer to withdraw money from an account using an ATM owned and operated by a financial institution other than the financial institution that holds the account.

10. The placement of skimming/access devices allows participants in these

fraud schemes to use devices to capture account information and PINs on terminals where victims use their credit and debit cards. The scheme participants then create counterfeit debit or credit cards and use the counterfeit cards and stolen PINs to obtain cash and other property from the victim's accounts.

11. A skimming device surreptitiously records account information from credit or debit cards while such cards are in use. Participants in the scheme typically install the device on, over, or inside a genuine card reader in such a way as to avoid detection by the card users. Card skimming/access devices can be found on debit/credit card readers located at ATMs, but also at point-of-sale terminals in retail stores, gas stations, or similar locations. In some instances, the device is used in conjunction with a camera either contained within the device or in a separate device. The camera is focused on the keypad of the machine and is capable of capturing images of the user's manual entry of their PIN. In other instances, the electronic components of the skimming device can record the PIN and a camera is not necessary.

12. Participants in the skimming/access device scheme typically remove the skimming device from the compromised machine after a short period of time. Participants in the scheme then transfer the stolen account information recorded from credit or debit cards from the skimming device to a computer or other electronic storage device. The participants then match that information with corresponding PINs. Participants in these schemes also use "Bluetooth" technology to transfer the stolen information via radio waves from the skimming device to a computer rather than using cables or wires to connect the skimming device and the computer. This technology allows



the criminals to surreptitiously download the stolen account information without the need to remove the skimming device from the compromised machine.

13. A counterfeit credit or debit card can be made by transferring a genuine card's account information to another card with a magnetic strip through the use of a magnetic strip encoding machine. Participants in the scheme may then use the counterfeit card with the corresponding PIN to fraudulently withdraw funds from a compromised bank account or at a business to fraudulently purchase goods and services.

### **PROBABLE CAUSE**

### **BACKGROUND OF THE INVESTIGATION**

14. In October of 2023, I became aware of an investigation into the placement of skimming devices on ATM machines operated by Bank Newport. The investigation was initiated on October 18, 2023, by the Bristol Police Department after they were contacted by Bank Newport personal regarding the discovery of a skimming device on a drive through ATM machine at a branch located in Bristol, Rhode Island.

15. Bank Newport provided surveillance footage and still images that clearly showed two males placing and removing devices from Bank Newport ATMs. Through my investigation, including discussions with law enforcement officers in various jurisdictions, including Warwick, Johnston, Coventry, Bristol, and elsewhere, I learned that at least one of the male subjects observed placing and removing skimming devices from the Bank Newport ATM, also placed skimming devices at retail locations in September and December of 2023.

16. In September of 2023, several police departments in Rhode Island and

Massachusetts received calls from retailers who discovered skimming devices attached to point-of-sale terminals in their stores. The retail locations that discovered these skimming devices include BJ's Wholesale Clubs in Johnston, RI (09/09/2023), Warwick (09/09/2023), and Seekonk, MA (09/09/2023), as well as in Walmart stores in Coventry, RI (09/09/2023), Walpole, MA (09/14/2023), Avon, MA (09/14/2023), and Raynham, MA (09/14/2023).<sup>4</sup> Several of these retailers captured security footage of individuals suspected of placing and in some cases removing these skimming devices on point-of-sale terminals.

17. On December 17, 2023, members of the Westerly Police Department were contacted following the discovery of numerous compromised accounts resulting from skimming devices that were placed at two branch Westerly Community Credit Union (WCCU) ATMs in Westerly, RI. In the Bristol and Westerly incidents, bank personnel provided security footage and still photographs of individuals who were likely responsible for the placement and removal of these skimming devices. They also provided footage and photographs of individuals withdrawing cash from many of the compromised accounts.

18. As part of my investigation, I collected skimming devices seized from police departments in Bristol, Warwick, Coventry, Johnston, and Seekonk. On January

---

<sup>4</sup> Walmart security personnel have alerted me to other incidents where skimming devices were located at point-of-sale terminals in various locations in Massachusetts in August and September of 2023. This affidavit will not cover all of these incidents but will instead focus mainly on those incidents in which skimming devices were recovered and turned over to HSI for further investigation.

26, 2024, U.S. Magistrate Judge Patricia A. Sullivan authorized a search warrant for a digital extraction of these five skimming devices and one mini digital camera. On February 8, 2024, I turned these devices over to a U.S. Secret Service Task Force Officer for analysis.<sup>5</sup>

19. A review of the security footage from the retailers and financial institutions impacted by the placement of these skimming devices has revealed that the Target Subjects and others are responsible for the placement of these devices in violation of 18 U.S.C. § 1029(b)(2), (conspiracy to commit access device fraud). Furthermore, Nicolas Longin CODREANU, Armando Ion CODREANU, and Ionut ZAMFIR illegally acquired and used victims' personal banking data stolen through the placement of these devices in violation of 18 U.S.C. § 1344 and 1349 (conspiracy to commit bank fraud) and 18 U.S.C. § 1028A(a)(1) and (c)(5) (aggravated identity theft).

### **THE RETAIL INCIDENTS**

20. As part of this investigation, I obtained security footage and images from Walmart and BJ's Wholesale Clubs in multiple jurisdictions. I have reviewed this footage and images and observed that Nicolas Longin CODREANU, Armando Ion CODREANU, Robby Vicson CODREANU, Isabela Ignat CODREANU, Mila CIUCIU,<sup>6</sup> and others were responsible for the deployment of skimming devices at multiple retail

---

<sup>5</sup> The forensic review of these devices is ongoing.

<sup>6</sup> A review of the retail incidents referenced herein did not show images of Ionut ZAMFIR engaged in the placement or removal of skimming devices at these retail locations. ZAMFIR was captured at financial institutions conducting similar activity that will be covered later in this affidavit.

locations across various jurisdictions. I have identified these subjects through my review of security footage from these incidents and compared this footage with photos of these individuals discovered in Department of Homeland Security (DHS) records, review of arrest reports, review of publicly available social media profiles, discussions with other law enforcement officers, and through DHS facial recognition tools.

21. The examples provided in this affidavit show that these six subjects work together in placing skimming devices on cash register terminals. These skimming devices are then used to capture the credit and debit cards of customers using these terminals. In some cases, the Target Subjects return to these same terminals and retrieve or attempt to retrieve these skimming devices.

22. Based on my conversations with loss prevention <sup>7</sup> personnel at BJ's Wholesale Club and Walmart, I learned that the breadth of the criminal activity perpetrated by the Target Subjects, exceeds the events described in detail here in Rhode Island and Massachusetts. For example, according to BJ's Wholesale Club, from May of 2023 through August of 2023, skimming devices were retrieved in 22 separate locations, including, Virginia, Maryland, New Jersey, New York, and Massachusetts. BJ's provided still images taken from security footage at the retail locations where these devices were retrieved. In many of these cases, the Target Subjects can be seen at these locations and at the point-of-sale terminals where the skimming devices were later found. Below are

---

<sup>7</sup> Personnel employed in the prevention of retail theft at the retailers referenced herein use various titles to describe their work. For ease of reference, these personnel will be referenced here as loss prevention.

several examples of BJ's Wholesale Club capturing the Target Subjects at these stores prior to the discovery of the skimming devices:<sup>8</sup>



Robby Vicson CODREANU, Nicolas Longin CODREANU and Mila CIUCIU at BJ's in Middle Village, NY – 7/15/2023 (Device found on 7/18/2023).



Armando Ion CODREANU at BJ's in Bronx, NY – 7/17/2023 (Device found on 7/17/2023).

---

<sup>8</sup> It should be noted that the surveillance photos provided by BJ'S Wholesale Club showed other individuals either with or without the Target Subjects entering or leaving stores prior to the discovery of the skimming devices. I believe that some of these other individuals were working with the Target Subjects in the deployment of skimming devices at these stores. This belief is based on the fact that these individuals could be seen checking out or walking with the Target Subjects in many instances. Furthermore, I also observed some of these unidentified subjects in social media photos along with the Target Subjects. However, not all of these unidentified subjects were present for the deployment of skimming devices in Rhode Island and will not be named in this affidavit.



Nicolas Longin CODREANU and Mila CIUCIU at BJ's in Brooklyn, NY – 7/17/2023 (Device found on 7/18/2023).



Armando Ion CODREANU at BJ's in Queens, NY – 7/17/2023 (Device found on 7/17/2023).



Nicolas Longin CODREANU and Mila  
CIUCIU at BJ's in Linden, NJ – 7/17/2023  
(Device found on 7/19/2023).



Nicolas Longin CODREANU and Armando  
Ion CODREANU at BJ's in Paramus, NJ –  
7/2/2023 (Device found on 7/18/2023).

Armando Ion CODREANU back at BJ's in  
Paramus, NJ – 7/17/2023 (Device found on  
7/18/2023).





Nicolas Longin CODREANU, Mila CIUCIU, and Robby Vicson CODREANU at BJ's in Paramus, NJ – 7/15/2023 (Device found on 7/18/2023).

Warwick, RI

BJ'S Wholesale Club

23. As part of this investigation, I obtained a Warwick Police report documenting the discovery of a skimming device on September 9, 2023, at the BJ's Wholesale Club located at 375 East Avenue in Warwick, RI. According to the report, upon arriving at the store, law enforcement met with BJ's loss prevention officer, J.P., and store manager, T.S. The report indicates T.S. was aware that BJ's locations in Seekonk and Johnston also discovered skimming devices at their stores. The report states J.P.



provided surveillance video of events that occurred on September 8, 2023, wherein two males and one female entered the BJ's and could be seen bringing merchandise to one of the self-checkout terminals. One of the males, wearing a baseball cap, could be seen removing a device from his torso area and placing it on top of the credit/debit card reader. The group then used an Electronic Benefits Transfer (EBT) card to purchase approximately \$80 in goods from BJ's. The report states that the BJ's membership ID used to make this purchase belonged to I.M. of Bowie, Maryland.<sup>9</sup> According to BJ's records, this is the same BJ's membership ID used to make numerous purchases by the Target Subjects while they were suspected of either placing or removing skimming devices at stores in Virginia, Maryland, New Jersey, New York, and Massachusetts as referenced above.

24. Based on a review of security footage, Warwick Police were able to determine that the three individuals believed to have placed the skimming device departed the BJ's in a blue Toyota Sienna van bearing Virginia registration TNP4406.<sup>10</sup> The below images depict the three individuals suspected of placing the skimming device on September 8, 2023, as well as the skimming device that was seized on September 9, 2023 from this terminal:

---

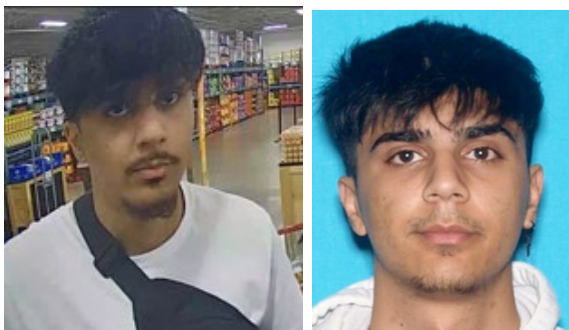
<sup>9</sup> Law enforcement and DHS records checks for the name I.M. at the address provided in Bowie, MD, did not result in any positive matches.

<sup>10</sup> According to police in Amelia County, VA, this vehicle bearing this license plate was towed on September 29, 2023, after being left at a business for five consecutive days, and likely abandoned.

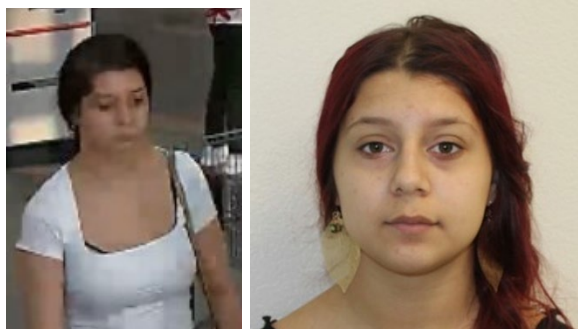




25. Based on my review of a driver's license photo for Armando Ion CODREANU and a DHS photo of Mila CIUCIU, I believe that these two assisted the individual in the white hat as he deployed this skimming device at the BJ's in Warwick on September 8, 2023. Although it is difficult to see the face of the individual in the white hat, based on my review of these photos and videos, as well as photos and videos from other incidents, I believe that this individual is likely Robby Vicson CODREANU. The images below show the three subjects at BJ's in Warwick in September of 2023 compared to other known photos of these subjects:



Armando Ion CODREANU at BJ's on 9/8/2023 and driver's license photo.



Mila CIUCIU at BJs on 9/8/2023 and DHS photo.



Robby Vicson CODREANU at BJs on 9/8/2023 and social media photo.

26. According to the Warwick Police report, BJ's reported that the suspects came to the same BJ's, driving the same vehicle (blue Toyota Sienna) on September 13, 2023, in a possible attempt to retrieve the skimming device (device with Property #23-2939-PR). I have reviewed surveillance video and still photos from the September 13, 2023, incident and observed that a male subject appears similar in appearance to one of the two males who were observed at the BJ's on September 8, 2023. This male subject wore what appears to be the same T-shirt and shoulder bag as Armando Ion CODREANU from September 8, 2023, but wore a baseball hat on September 13<sup>th</sup>. Upon closer review of the security footage from this date, it appears that this male was Robby Vicson CODREANU. The female subject present on September 13<sup>th</sup> was not the same



female subject who arrived at the BJ's on September 8<sup>th</sup>. This female also wore a baseball cap. However, based on my review of the surveillance footage from September 13<sup>th</sup>, I believe that the female present on this date was Isabela Ignat CODREANU. Below are still images of the two suspects at the same point-of-sale terminal at BJ's on September 13, 2023, as well as a DHS photo of Isabela Ignat CODREANU and an April 2024 arrest photo of Robby Vicson CODREANU:



Robby Vicson CODREANU and Isabela Ignat CODREANU at BJ's on 9/13/2023.



Isabela Ignat CODREANU at BJ's on 9/13/2023 and a DHS photo.



Robby Vicson CODREANU at  
BJs on 9/13/2023 and an April  
2024 arrest photo.

### Walmart

27. According to a police report I obtained from the Warwick Police Department, on January 23, 2024, they were called to the Walmart located at 840 Post Road for a report of the discovery of a skimming device on one of their registers. According to the report, Walmart loss prevention associate S.M. informed them that the device was first discovered by an employee on January 18, 2024, on self-checkout aisle #51. S.M. stated that she reviewed security footage and discovered that the skimming device was installed on December 16, 2023, at approximately 1714 hours (5:14 PM).

28. Walmart employee S.M. provided Warwick Police with the skimming device and a copy of security footage from December 16, 2023, the date she believed the device was put in place. Warwick Police provided me a copy of this security footage, which I have reviewed. In this footage, I observed a male place the skimming device on the point-of-sale terminal at approximately 5:14 PM, while a female and another male stand alongside of him, as seen below:



29. After placing the device, the male paid cash for a purchase of multiple food and drink items and departed the area. Walmart provided law enforcement with security footage of this incident taken from multiple camera angles. I have reviewed these surveillance videos and determined that Nicolas Longin CODREANU placed this skimming device, while Isabela and Armando stood watch at register #51. More specifically, Isabela Ignat CODREANU appears to stand next to Nicolas and watch him place the skimming device on the terminal as she checks out items as seen below:



30. Below is a still image taken from one of these surveillance videos showing the trio at the Walmart in Warwick on December 16, 2023, prior to the placement of the skimming device:





Isabela, Nicolas, and Armando CODREANU at Walmart on 12/16/2023.

31. Although Nicolas Longin CODREANU is wearing a blue-colored surgical type mask during this incident, I believe that this is Nicolas Longin CODREANU based on my review of him appearing in numerous other videos and based on him wearing the

same unique grey sweatpants that he wore in October while placing skimming devices on Bank Newport ATMs in Rhode Island. These sweatpants have a Nike logo on the left side and an unusually large, black-colored pocket on the right leg of these sweatpants as seen below:



Nicolas Longin CODREANU at Walmart on 12/16/2023 and Bank Newport ATMs on October 16-17, 2023.

32. According to a Warwick Police report, on January 24, 2024, police were dispatched to Walmart where an employee, L.G., reported that she used her Bank of America credit card to make a purchase at Walmart (while the skimming device was in place at register #51). L.G. reported that on January 24, 2024, Bank of America notified her of fraudulent activity on her card, where a purchase of \$198.78 was made at a business called "PowerMax."<sup>11</sup> L.G. stated that she was still in possession of her card but believes

---

<sup>11</sup> An online search of the term "PowerMax" reveals multiple products and retailers such as auto parts and athletic gear using this same name.

that this purchase was made fraudulently as a result of someone accessing her credit card information through the skimming device that was discovered in this store.

Johnston, RI

33. I spoke with Johnston Police Detective Derek Parascandolo who informed me that their department was also investigating an incident where three individuals placed a skimming device on a point-of-sale terminal located at the BJ's Wholesale Club in Johnston, RI. Detective Parascandolo provided me a copy of the police report documenting this incident. I reviewed this report and learned that on September 9, 2023, Johnston Police responded to the BJ's located at 200 Stone Hill Drive in Johnston and, upon arrival, met with the store manager, J.C., who informed them that on that date he received information from BJ's loss prevention officer, T.M., that a group of individuals had been installing skimming devices at BJ's stores. Upon hearing this, J.C. checked all of the Johnston BJ's cash registers and located a skimming device affixed to self-checkout #20 (register #83). J.C. removed the device and turned it over to Johnston Police.<sup>12</sup>

34. BJ's provided Johnston Police with video surveillance footage from September 8, 2023. The police report indicates Detective Parascandolo reviewed this video footage and determined that at approximately 6:37 PM, two males and one female approached the self-checkout register at which the skimmer was found. Detective Parascandolo reported that while the group was at the register, the female and one of the male suspects appeared to be blocking the view of the terminal as the second male

---

<sup>12</sup> This skimming device was seized by Johnston Police and bears property # 23-1977-PR.

appeared to manipulate the credit card terminal prior to paying for various items. Detective Parascandolo has since shared a copy of this footage with me. I reviewed this footage and still images and observed that the three individuals at the register in the Johnston BJ's appear similar to the three who were observed at the Warwick BJ's earlier that same day, Armando Ion CODREANU, Robby Vicson CODREANU, and Mila CIUCIU. Below is an image of the three departing the BJ's in Johnston after spending several minutes at the register where the device was recovered:



Coventry, RI

35. According to a police report I received from the Coventry Police Department, on September 9, 2023, they were called to the Walmart located at 650 Centre of New England Blvd. in Coventry regarding the reported discovery of a skimming



device at one of the store's self-checkout point-of-sale terminals. According to the report, J.V., a Walmart employee, met police upon their arrival and provided video surveillance footage of two males and one female who were observed on September 8, 2023, the previous day, at the self-checkout aisle where the skimming device was found. The video footage, according to the report, clearly shows one of the male subjects remove a skimming device from his coat and place the device over the self-checkout register. As he places the device on the register, the second male and the female can be seen on either side of him holding up items in an apparent attempt to conceal his activities. Despite their efforts, the security camera above them captured their placement of the skimmer:<sup>13</sup>



36. Other security footage captured the trio while walking in the store and their

---

<sup>13</sup> It appears that Armando Ion CODREANU and Mila CIUCIU used a jacket and a reusable Walmart bag, respectively, to shield Robby Vicson CODREANU from the view of potential on-lookers while he installed the skimming device and, once installed, no one in the group purchased the jacket or reusable bag and both items were left behind when the trio left the store.

vehicle as they exited the parking lot. The vehicle, a blue Toyota Sienna, is the same vehicle and registration observed at the BJ's in Warwick on this same date. I reviewed photographs of this footage and determined that these three subjects are Robby Vicson CODREANU, who placed the device, along with Mila CIUCIU and Armando Ion CODREANU, who stood on either side of Robby shielding his activities from view as the device was placed. These three placed the skimming devices at the BJ's in Warwick, Johnston, and Seekonk on this same date. Surveillance photos of these three subjects and their vehicle at the Coventry Walmart can be seen below:



#### Seekonk, MA

37. According to the Seekonk Police Department, on September 9, 2023, they were called to the BJ's located at 175 Highland Avenue for the reported discovery of a skimming device. A Seekonk Police report documenting the incident states police met with a BJ's employee, J.F., who said she received a call from BJ's loss prevention officer, T.M., who informed her about the other skimming incidents and requested that she check the registers. The police report indicates J.F. said she discovered the skimming device

affixed to one of the self-checkout registers (register #84), removed it, and contacted the police.

38. The police report indicates J.F. reviewed video surveillance footage from the previous day (09/08/2023) and observed two males and one female approach register #84. While at the register, one of the males and the female could be seen shielding the terminal as the second male appeared to affix the skimming device to the register. The subjects used an EBT card to purchase several items and departed the store. BJ's provided surveillance footage and still photographs of the three individuals, who appear below. Based on my review of the footage, these three individuals are Mila CIUCIU, Armando Ion CODREANU, and Robby Vicson CODREANU.









### Compromised EBT Card Used by the Target Subjects

39. Based on the discovery of these skimming devices at the various retail locations, I requested records from Walmart for information about the cards that were used while these devices were in place at the point-of-sale terminals. Walmart was able to isolate their search to the specific terminals and time frames when the skimming devices were in place. According to Walmart records, nearly 5,000 credit/debit and EBT cards were run through the point-of-sale terminals while skimmers were in place at Walmart stores in Warwick and Coventry. Additionally, Walmart identified more than 9,000 cards that were run through terminals where the Target Subjects installed skimmers at Walmart stores in Massachusetts (Quincy, North Attleboro, Raynham, and Avon).<sup>14</sup>

40. I discovered that among the cards used to make purchases at the various Walmart stores while the skimming devices were in place were hundreds of Electronic Benefit Transfer (EBT) Cards.<sup>15</sup> One of these EBT cards, ending in 0148, was used to make a purchase at the Walmart in Warwick on January 14, 2024, at the terminal where the skimmer was placed by Nicolas Longin CODREANU, Armando Ion CODREANU, and Isabela Ignat CODREANU on December 16, 2023. This EBT card is associated with a 65-year-old female Supplemental Nutritional Assistance Program (SNAP) recipient based in Warwick, RI, hereinafter referred to as O.P. According to Walmart, this same EBT card

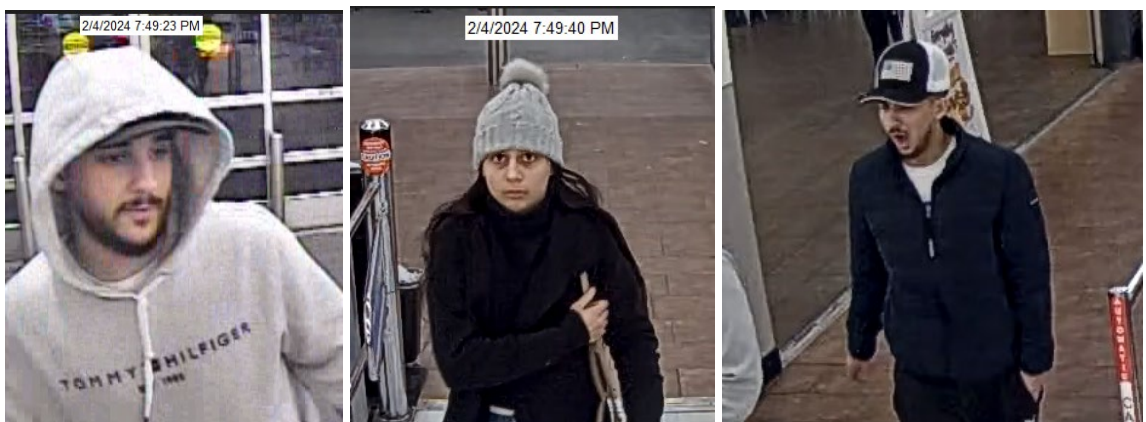
---

<sup>14</sup> Walmart also informed me that the Target Subjects were involved in multiple other incidents where they were captured on video surveillance placing skimming devices on point-of-sale terminals in various states. Not all of these incidents will be covered here.

<sup>15</sup> According to the U.S. Department of Agriculture, EBT cards allow qualifying participants of the Supplemental Nutrition Assistance Program (SNAP) to pay for food using SNAP benefits (<https://www.fns.usda.gov/snap/ebt>).

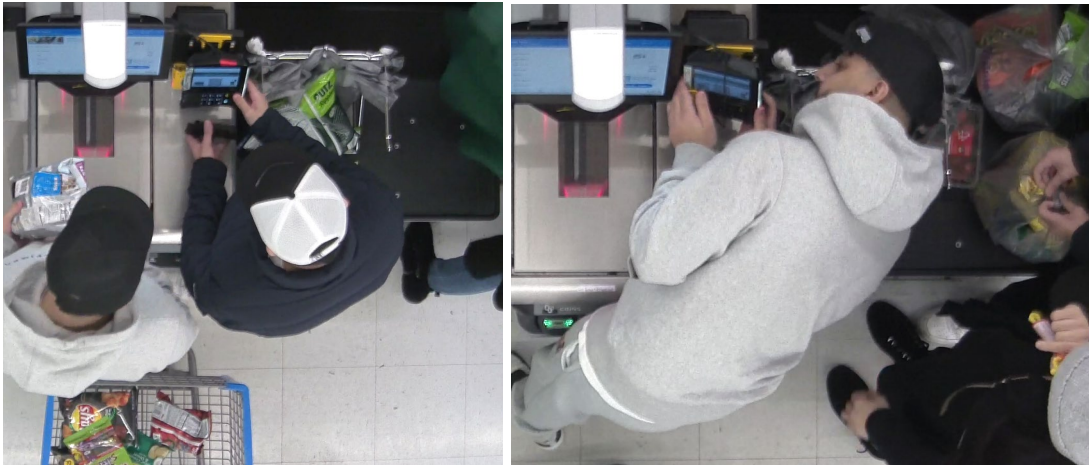
was used again on February 4, 2024, to make several purchases at two Walmart stores located in York, PA. Walmart provided security footage from the times when these cards were used at both York stores on February 4, 2024. This footage shows that in both cases, Nicolas Login CODREANU, Robby Vicson CODREANU, and Mila CIUCIU make these purchases. This footage also shows that the trio placed skimming devices at point-of-sale terminals in both stores as they use a cloned EBT card skimmed from O.P. of Warwick, RI.

41. I reviewed Walmart security footage from February 4, 2024, taken at the store located at 1000 Town Center Drive, in York, PA. According to Walmart records, two males and one female entered the store and worked in tandem, while one of the males placed a skimming device on register #50. Walmart provided videos and photos of this trio. I have reviewed these photos and videos and positively identified the three as Nicolas Longin CODREANU, Robby Vicson CODREANU, and Mila CIUCIU. Images of these three taken on February 4, 2024, at the York Walmart at 100 Town Center Drive appear below:



Nicolas Longin CODREANU, Mila CIUCIU, and Robby Vicson CODREANU at Walmart in York, PA on 2/4/2024.

42. Walmart security footage shows the trio approach register #50. Once at the register, Nicholas Longin CODREANU manipulates the pin pad and removes it from its base as Mila CIUCIU holds up a t-shirt in an apparent attempt to block the view of this activity. Once the pin pad is dislodged from its base, Nicolas Longin CODREANU and Robby Vicson CODREANU switch places. Nicolas then began scanning food items while Robby removes a skimming device from his right front coat pocket and place it over the pin pad as seen below:



43. After the device is put in place, Nicolas then assists Robby with putting the pin pad bank in place. During this entire process, Mila CIUCIU holds up a green-colored t-shirt<sup>16</sup> blocking the side view of the terminal. Once the trio are done checking out their items, Nicolas holds his hand out to Robby who then hands him a blue-colored Visa gift

---

<sup>16</sup> No one in the group purchased this t-shirt and it was discarded in the bagging area next to register #50.

card that Nicolas uses to make the purchase of these items. Nicolas entered in a pin for the card and received a receipt for their purchase. Seemingly unsatisfied with the placement of the skimming device, Nicolas then continued to make numerous adjustments to the pin pad by removing it from its base and attempting to replace the terminal. While he was doing this, Robby stepped back next to Nicolas and purchased multiple other candy and gum items as Mila CIUCIU looked on, as seen below:



44. Nicolas and Robby continued to make adjustments to the pin pad terminal before Robby paid for the candy and gum items using what appeared to be the same blue Visa gift card.

45. Walmart provided receipts for these purchases, which show checkout times

of 7:55 PM and 7:58 PM at register #50, as seen below. This date and time frame match the date and time frame from the Walmart surveillance images that captured Nicolas Longin CODREANU, Robby Vicson CODREANU, and Mila CIUCIU checking out at this register.<sup>17</sup>

**Walmart**   
Save money. Live better.  
WAL\*MART  
YORK, PA  
ST# 2205 OP# 9050 TE# 50 TR# 3229

DORITOS COO	002840032504 F	2.48
HST SS HNYB	088810925309 F	1.58
LAYS	002840032382 F	2.48
7.75OE SCO	004178027187 F	2.94
SPK FF	007046200659 F	1.28
KISSES MC	003400013480 F	13.24
TWIN SNAKES	004223834093 F	1.28
DORITOS	002840032505 F	2.48
LAYS BBQ	002840032420 F	2.48
LAYS	002840032421 F	2.48
SMTF RAINBO	002840033179 F	2.48
MRGOODBARKL	003400017315 F	2.16
TOPPS JCY D	004111600592 F	2.28
TIC TAC T20	000980000630 F	3.98
REESES	003400043227 F	4.84
7.75OE BBQ	004178027166 F	2.94
STRAWBERRIE	085487700701 F	2.98

SUBTOTAL 54.38  
TAX 12 0 % 0.00  
TOTAL 54.38  
EBT SNAP TEND 54.38  
ACCOUNT # \*\*\*\* \* 0148  
CHANGE DUE 0.00

EBT SNAP  
54.38 TOTAL PURCHASE  
ACCOUNT # \*\*\*\* \* 0148  
APPROVAL CODE 041536  
BEG BAL END BAL  
EBT CASH 0.00 0.00  
EBT SNAP 131.35 76.97  
02/04/24 19:55:03

**# ITEMS SOLD 17**  
TC# 8331 2202 6033 1760 6212  
  
02/04/24 19:55:17

**Walmart**   
Save money. Live better.  
WAL\*MART  
YORK, PA  
ST# 2205 OP# 9050 TE# 50 TR# 3231

GUM	003400000545 F	4.12
MMALBUMPNT	004000000432 F	2.28
GUM	007339001405 F	4.12
MMALBUMPNT	004000000432 F	2.28
MMALBUMPNT	004000000432 F	2.28
MMALBUMPNT	004000000432 F	2.28
MMALBUMPNT	004000000432 F	2.28
MMALBUMPNT	004000000432 F	2.28
MMALBUMPNT	004000000432 F	2.28

SUBTOTAL 21.92  
TAX 12 0 % 0.00  
TOTAL 21.92  
EBT SNAP TEND 21.92  
ACCOUNT # \*\*\*\* \* 0148  
CHANGE DUE 0.00

EBT SNAP  
21.92 TOTAL PURCHASE  
ACCOUNT # \*\*\*\* \* 0148  
APPROVAL CODE 051319  
BEG BAL END BAL  
EBT CASH 0.00 0.00  
EBT SNAP 76.97 55.05  
02/04/24 19:58:11

**# ITEMS SOLD 8**  
TC# 3855 5995 1988 7510 1535  
  
02/04/24 19:58:22

46. As these receipts show, both purchases were made using O.P.'s EBT card ending in 0148. I reviewed a government photo of O.P. and can confirm that she was not present when these purchases occurred at the Walmart in York. Further, I have reviewed multiple online photos of RI EBT cards, issued by the RI Department of Human Services

<sup>17</sup> Although the surveillance videos provided by Walmart do not have date and time stamps, the still images provided by Walmart taken from these videos do list the date and time that match the date and time frame for these receipts.

and determined that these cards are not similar in appearance as the Visa gift card used by Nicolas and Robby CODREANU in York, PA. Based on these facts, I believe that in this case, Nicolas Longin CODREANU fraudulently used O.P.'s SNAP benefits to make these purchases through the use of a cloned EBT card.

47. On February 6, 2024, Walmart personnel discovered and removed this device, which can be seen below:



48. According to Walmart, O.P.'s EBT card ending in 0148 was used to make a purchase at a second Walmart in York, PA on the same date (2/4/2024). According to Walmart, on February 4, 2024, at approximately 8:21 PM, O.P.'s EBT card was used to purchase 17 items at register #49 located at the Walmart at 2801 E Market Street, York, PA. Walmart provided a copy of this receipt as seen below showing the card number ending in 0148:





WAL\*MART  
YORK, PA  
ST# 1529 OP# 9049 TE# 49 TR# 4115

POP WT CHED	002840063769 F	2.50
CHEETOS	002840032949 F	2.48
DORITOS CR	002840068877 F	2.48
SNACKS	075752804807 F	1.98
KING SIZE	003400000229 F	2.28
KINDER BUEN	000980000055 F	1.46
POP SEASLTV	002840030695 F	2.50
KING SIZE	003400000480 F	2.28
LAYS	002840067474 F	2.50
ICE BREAK	003400000098 F	2.82
LAYS BBQ	002840019961 F	2.50
KINDER BUEN	000980000055 F	1.46
EXTRA GUM	002200000899 F	1.38
MINT	003400000665 F	2.82
KINDER BUEN	000980000055 F	1.46
MINT	003400000665 F	2.82
BEESWAX BAL	079285011000	3.58

SUBTOTAL		39.30
TAX 1	6 %	0.22
TAX 12	0 %	0.00
TOTAL		39.52
EBT SNAP TEND		35.72
ACCOUNT #	**** * 0148	
CASH TEND		10.00
CHANGE DUE		6.20

EBT SNAP  
35.72 TOTAL PURCHASE  
ACCOUNT # \*\*\*\* \* 0148  
APPROVAL CODE 008143  
EBT CASH 0.00 0.00  
EBT SNAP 55.05 19.33  
02/04/24 20:20:50

# ITEMS SOLD 17

TC# 6676 9575 3881 8996 1516



02/04/24 20:21:58

49. Walmart provided video surveillance of this purchase which shows Robby Vicson CODREANU and Nicolas Longin CODREANU both unsuccessfully attempting to remove a yellow-colored security tab placed over the point-of-sale terminal as Nicolas Longin CODREANU purchases items and Mila CIUCIU stands nearby. An image from this footage can be seen below:



50. When Nicolas Longin CODREANU pays for the items, he deposits \$10 cash for the purchase and appears to again use a “Vanilla Go” Visa gift card for the remaining balance, as seen below:



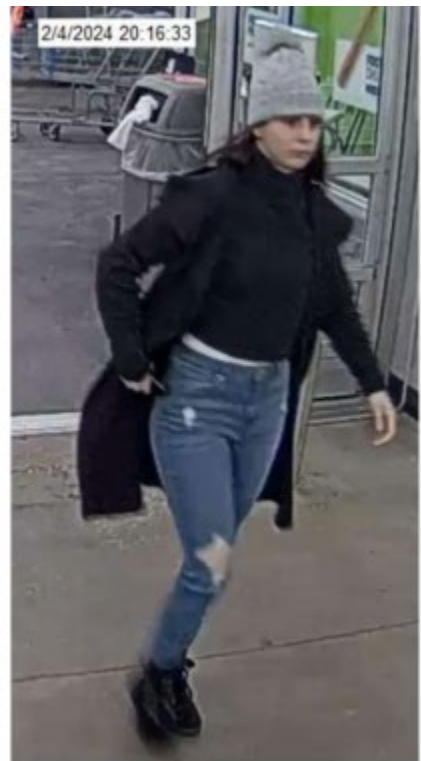


51. As previously stated herein, I have learned from this investigation and from conversations with other law enforcement officers that when a skimming device captures data from an EBT card, this data can then be cloned, using another card with a magnetic strip such as the Vanilla Go gift card used by Nicolas Longin CODREANU here. Based on the information, I believe that Nicolas Longin CODREANU used the skimmed information from O.P.'s EBT card to make this purchase at register #49 at the York Walmart.

52. Based on my review of Walmart security footage of this incident and my conversations with Walmart security manager M.S., I believe that after the Target Subjects were unsuccessful in placing the skimming device at register #49, they moved to register #51. My review of security footage from register #51 shows Nicolas Longin CODREANU, Robby Vicson CODREANU, and Mila CIUCIU making an additional purchase at this same Walmart on February 4, 2024. This footage also shows Robby Vicson CODREANU successfully installing a skimming device over the point-of-sale terminal on register #51. Robby Vicson CODREANU made a purchase of food items at register #51 using what appears to be another Visa gift card. On February 7, 2024, Walmart discovered and removed this skimming device from register #51. Images of Robby Vicson CODREANU installing this device while Nicolas Longin CODREANU and Mila CIUCIU stand next to him at this Walmart on E. Market Street in York, PA on February 4, 2024:



Robby Vicson CODREANU installing skimming device at Walmart on E. Market Street in York, PA on 2/4/2024.



Nicolas Longin CODREANU, Robby Vicson CODREANU, and Mila CIUCIU at Walmart on E. Market Street in York, PA on 2/4/2024.



Skimming devices discovered by Walmart personnel at register 51 at the E. Market Street Walmart in York, PA on 2/7/2024.

## **THE BANK INCIDENTS**

### **Bank Newport – Bristol/Warren/Johnston, RI**

53. As previously referenced herein, on October 18, 2023, the Bristol Police Department responded to a report of the discovery of a skimming device at Bank Newport located at 6 Gooding Avenue in Bristol. I obtained a copy of the Bristol Police report documenting this incident. According to this report, Bristol Police spoke with Bank Newport employee K.L., who informed them that she discovered the devices after a customer complained about not being able to insert his/her bank card into the ATM. While on the scene, Bristol Detectives John Nappi and Tim Kearns also met with Bank Newport employee N.T. and examined the ATM. The detectives and N.T. discovered two devices affixed to the drive through ATM. Bristol Police described these devices as a chip reader and camera device (devices bearing property #s 23-355-PR and 23-356-PR).

54. Bristol Police received video surveillance footage from Bank Newport documenting several incidents in which suspects were observed installing this skimming

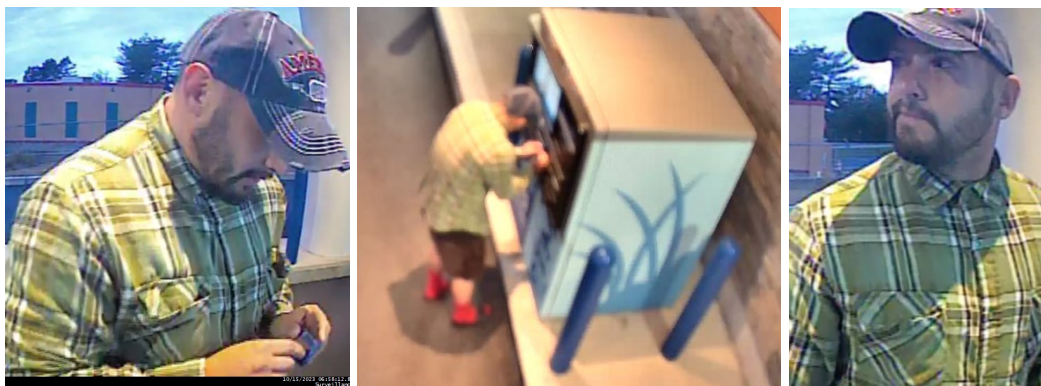
equipment onto the bank's ATM machine and footage of suspects then using compromised bank cards to withdraw cash at various Bank Newport ATMs. I reviewed these videos and photos and determined that the two suspects are Nicolas Longin CODREANU and Ionut ZAMFIR. The first security footage of Nicolas Longin CODREANU and ZAMFIR manipulating Bank Newport ATMs occurs on October 13, 2023. However, according to Bank Newport records, theft of funds from their customer's accounts did not occur until October 19, 2023.

55. The first available footage was taken on October 13, 2023, when two individuals I believe to be Nicolas Longin CODREANU and ZAMFIR approach the drive-through ATM at the Johnston, RI branch on foot at night. During this incident, ZAMFIR appears to make an adjustment to the ATM and CODREANU then removes a long thin object closely resembling the metal strip containing a hidden camera device seized by Bristol Police on October 18, 2023 (property #23-356-PR). After removing this device, CODREANU places the metallic looking strip into his sweatshirt and the two men walk away. An image of this incident in Johnston can be seen below:



56. On October 15, 2023, ZAMFIR was back at this same Bank Newport ATM in Johnston, RI. While at the ATM for several minutes, ZAMFIR appeared to make adjustments to the ATM while periodically checking his surroundings. At one point ZAMFIR appears to remove a small unidentified component from the ATM, inspect the component, and then replace this component back onto the ATM. ZAMFIR then appears to conduct or attempt to conduct a transaction at the ATM before departing the area. Images of ZAMFIR conducting this activity can be seen below:





57. On October 16, 2023, Bank Newport security footage captured ZAMFIR as he placed a long metallic device believed to have contained a video camera onto the ATM at the Warren branch. ZAMFIR then appeared to make an adjustment to the ATM or possibly place an unidentified component onto the ATM's card slot area. ZAMFIR then conducted a test on the ATM's card slot by inserting what appeared to be a debit or gift card containing a Visa symbol and then removing this card. ZAMFIR then appeared to insert a small tool into the ATM's card slot area and made additional adjustments before departing the area on foot. Photos of ZAMFIR placing this device and making adjustments to the Warren Bank Newport ATM appear below:







58. On October 16, 2023, Bank Newport security footage reveals that later that day, Nicolas Longin CODREANU returned to this same ATM in Warren and used a tool to remove a blue-colored device from the ATM's card reader and place this device in his pocket. Nicolas Longin CODREANU then further manipulated the ATM and removed the metallic strip from the machine and placed this in his sweatpants. Based on this investigation, and as previously referenced herein, I believe that this metallic strip likely contained a mini camera that captured ATM user's PINs and card numbers. CODREANU then departed the area on foot. Images from this incident, including the tool CODREANU used and the device he removed from the ATM appear below:



59. Bank Newport provided another video dated October 17, 2023, that shows Nicolas Longin CODREANU and ZAMFIR approach the drive-through ATM in Bristol on foot. CODREANU can be seen removing a similar metallic strip from his sweatshirt and place it on the ATM. CODREANU then manipulates the ATM, while ZAMFIR stands watch over him. CODREANU then inserts a card into this ATM before the two subjects depart the area on foot. Photos of Nicolas Longin CODREANU and ZAMFIR at the Bristol ATM on October 17, 2023, appear below:



60. On October 17, 2023, Bank Newport security footage showed that ZAMFIR returned to the Warren ATM where he made an adjustment to the ATM before entering what appeared to be a debit/gift card with a Visa logo into the machine multiple times. ZAMFIR then looks around and removes what appears to be a small forceps-type tool from his shirt pocket, bend down and make several adjustments to the ATM's card slot area. ZAMFIR then appeared to blow into the card reader slot before departing the area.

Photos of this incident appear below:



61. In another Bank Newport video from the Bristol branch dated October 18, 2023, the date of the discovery of the skimming device at this branch location, Nicolas Longin CODREANU can be seen driving up to the drive-through ATM machine in a red Jeep Grand Cherokee. There appears to be a female in the passenger seat of the vehicle. Nicolas Longin CODREANU can be seen removing a similar metallic strip from the vehicle and placing it on the ATM. The female then hands Nicolas Longin CODREANU a small unidentified object that he appears to place on the ATM. CODREANU then

makes several manipulations to the ATM and appears to conduct or attempt to conduct a transaction using a card before the two drive away. Based on the timing of this incident, I believe that this video footage depicts CODREANU placing the skimming device and metallic strip containing the camera that were discovered by Bank Newport later that day. Below are several photos of Nicolas Longin CODREANU placing this metallic strip at the Bristol ATM:



62. On multiple occasions, I spoke with K.F., a Fraud and Security Officer at Bank Newport, who provided information about the impact of these skimming devices on their financial institution and its customers. In total, K.F. stated that 12 customer bank cards were compromised as a result of the placement of the skimming device in Warren and 96 cards were compromised at the Bristol branch. Of these compromised cards, 22 customer accounts reported unauthorized transactions against their accounts totaling more than \$17,000. I reviewed these customer accounts and discovered that all 22 customers who reported unauthorized withdrawals from their accounts are residents of Rhode Island.

63. These unauthorized transactions all took place on October 19, 2023, at the

Bank Newport Warren ATM. Bank Newport provided video footage of these unauthorized transactions being conducted. I reviewed these videos and determined that Nicolas Longin CODREANU conducted these transactions at the Warren ATM. According to the date and time stamps on the videos, Nicolas Longin CODREANU pulled up to the Warren drive through at approximately 5:42 AM in a small, black-colored BMW sport utility vehicle. CODREANU, who was wearing a black colored-hat and jacket, was driving while an unidentified person sat in the passenger seat and handed him multiple cards as he conducted the unauthorized transactions. After each transaction, Nicolas Longin CODREANU appeared to hand the card and withdrawn cash to the unidentified passenger in the front seat of the vehicle. Although not all of the cards used by CODREANU could be seen, some were partially visible in the video. These cards did not appear to contain any Bank Newport emblems. Instead, the visible cards appeared to resemble debit/gift cards commonly available for purchase at retail locations. Some of these cards contained the word Visa in the lower right corner of the card.

64. After conducting numerous transactions using different cards, Nicolas Longin CODREANU reversed the vehicle out of the ATM drive through lane at approximately 6:08 AM. He then drove to a second drive through ATM lane.<sup>18</sup> The video surveillance captured the black vehicle pulling into this second lane for the drive through ATM and continue conducting a similar pattern of activity, where Nicolas Longin

---

<sup>18</sup> The Bank Newport Warren branch has three separate drive through lanes.



CODREANU uses multiple cards to conduct ATM transactions and then hands those cards and withdrawn cash to the unidentified individual in the passenger seat. The passenger appears to package up the cash and card individually and made notations with a pen or similar writing utensil. At approximately 6:30 AM, an unidentified female wearing a grey hooded sweatshirt, dark baseball cap, and jeans could be seen exiting from the passenger side of the black vehicle and walking back to the original ATM machine, where she conducted or attempted to conduct a transaction using a card bearing the word Visa on the bottom right-hand corner. This female then returned to the black vehicle's passenger side at approximately 6:32 AM.

65. According to Bank Newport records, the unauthorized transactions all occurred on October 19, 2023, at the Warren branch between the approximate times of 5:42 AM and 6:43 AM, using 22 separate cards. The surveillance footage of the Warren Bank Newport branch ATMs shows nobody other than Nicolas Longin CODREANU and his unidentified female companion at this location during this time frame.

66. Bank Newport reported that as a result of this scheme and unauthorized withdrawals, they lost \$17,925.

67. Some images from the video footage from October 19, 2023, which captured the unauthorized withdrawals appear below:





Westerly Community Credit Union (WCCU) – Westerly, RI

68. On December 20, 2023, I became aware of an incident in which the WCCU discovered that several of their branch locations had been victimized by the installation of skimming devices on their ATMs. I have since obtained a copy of the Westerly Police Department's report documenting this incident as well as bank security footage and still images documenting several suspects believed to be responsible for the deployment of these devices and the depletion of victims' accounts. Although no skimming devices were recovered from these Westerly incidents, the activity will be documented herein because, based on a review of bank security footage, I believe that two of the suspects in these WCCU incidents are Target Subjects Ionut ZAMFIR and Armando Ion CODREANU. In total, WCCU reported the suspected deployment of skimming devices at two WCCU locations in Westerly, followed by unauthorized withdrawals from five WCCU branches located in Rhode Island as well as unauthorized withdrawals from WCCU accounts conducted from ATMs at two other banks (Berkshire Bank and Navigant Credit Union).

69. According to the Westerly Police report, on December 17, 2023, they were dispatched to the home of S.A. and C.A., an elderly couple in Westerly, RI, for a report of fraud.<sup>19</sup> According to Westerly Police, S.A. reported that while reviewing his account

---

<sup>19</sup> Note: In my affidavit submitted on January 26, 2024, seeking authorization to search 6 skimming devices, I stated that Westerly Police initially responded to WCCU on December 17, 2023. However, I have since learned that on December 17, 2023, Westerly Police initially responded to the home of S.A. and C.A. and later met with WCCU personnel at the Westerly Police Department and not at WCCU on that same date.

online, he observed multiple \$1000 ATM withdrawals from the branch located at Dunns Corners (244 Post Road) in Westerly. The customer then checked his wife's account and observed similar activity. In total, \$25,000 was withdrawn from both accounts.

70. According to the Westerly Police report, the bank contacted the police and made them aware of multiple complaints from customers who also reported fraudulent account activity. According to a statement made by M.S. of the WCCU, she believed that these fraudulent transactions were the result of a skimming device that was used to capture customers' card information, allowing the suspects to create new cloned cards with the same information which they then used to make withdrawals.

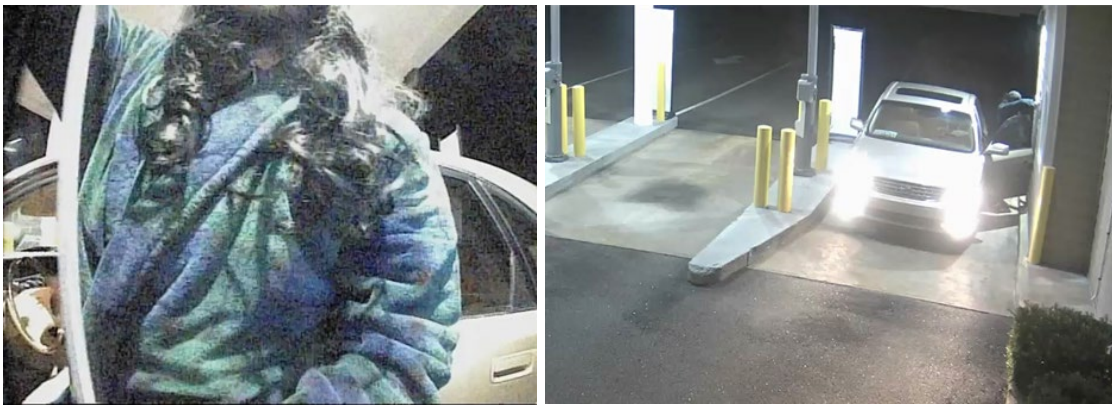
71. I have since spoken with WCCU personnel who provided copies of surveillance footage and images of several suspects who appear to install devices onto Westerly WCCU branch ATMs located on Post Road and Granite Street in Westerly on December 15, 2023.

72. Based on my review of images captured from the WCCU drive through ATM located at 244 Post Road in Westerly on December 15, 2023, I believe that on this date, beginning at approximately 6:04 AM, an individual I know to be Ionut ZAMFIR approached a drive through ATM as the sole occupant of a light-colored sedan. ZAMFIR exited the vehicle and inserted what appears to be a Visa gift card into the ATM's card reader. At the time, ZAMFIR was wearing a blue/green-colored bathrobe, black-colored hat, and long-haired wig as seen below:





73. At approximately 6:05 AM, ZAMFIR appeared to place a skimming device or part of a skimming device onto this ATM. This included a long metallic strip, similar in appearance to the one ZAMFIR and Nicolas Longin CODREANU installed at the Bank Newport ATM in October. ZAMFIR then drove away from the area. Images of ZAMFIR installing this device can be seen below:



74. Later that same date of December 15, 2023, at approximately 5:12 PM, bank surveillance images captured a male unknown to this investigation, pull up to this same drive through ATM on Post Road in Westerly and appear to remove the skimming device. Images of this unidentified male, wearing a hat and surgical-type facemask, can be seen below removing this skimming device and long metallic strip that likely contained a pinhole camera:



75. WCCU also provided footage and still images of other individuals who appear to install a skimming device on an ATM at the branch located at 122 Granite Street in Westerly. According to WCCU personnel, this incident occurred at approximately 12:42 AM on December 15, 2023. I reviewed this security footage and still images and determined that the individual responsible for the installation of this skimming device was likely I.P., a Romanian national and associate of Nicolas Longin CODREANU. Images from this installation appear below:



76. During this installation, I.P. was operating a dark-colored Volvo SUV. The passenger seat of this vehicle was occupied by another unidentified male.

77. WCCU provided still images of another unidentified male remove this

skimming device from the ATM located at 122 Granite Street later this same date at approximately 6:49 PM, in what video shows to be the same dark-colored Volvo SUV. This unidentified male exited the Volvo, removed the skimming device, and depart the area. Surveillance still images of the removal of this device can be seen below:



78. In addition to the installation and removal of the skimming devices, WCCU also provided still images taken from surveillance footage from the unauthorized withdrawals from WCCU victim accounts. I reviewed these images and determined that two of the individuals responsible for these unauthorized withdrawals are Ionut ZAMFIR and Armando Ion CODREANU.

79. As stated herein, all the unauthorized withdrawals from the compromised WCCU accounts occurred on December 17, 2023. According to WCCU, these withdrawals occurred at various ATMs in Rhode Island totaling \$279,250 stolen from 44 separate accounts.<sup>20</sup>

---

<sup>20</sup> WCCU originally reported 141 compromised accounts resulting from the placement of these skimming devices. WCCU analysis provided to me as part of this investigation shows 44 cards from these compromised accounts were likely cloned and used to conduct unauthorized withdrawals from compromised accounts.



80. WCCU reported that on December 17, 2023, their Dunn's Corner Branch (Westerly) ATMs (walk up and drive through ATMs) were used to make a total of \$117,050 in unauthorized withdrawals from 20 compromised accounts between the times of 4:28 AM through 7:18 AM. However, WCCU was only able to produce images from surveillance footage at the drive through ATM, which accounted for \$52,250 of these withdrawals from six accounts (including S.A's account who originally reported this incident to Westerly Police Department). These withdrawals occurred at this drive through ATM from 4:55 AM through 7:18 AM. I reviewed these images, which show ZAMFIR and Armando Ion CODREANU conducting these unauthorized withdrawals. Further, at least one of these images show ZAMFIR conducting transactions using a Visa gift card, which was likely used to clone a WCCU victim's card, based on what I have learned during this investigation. Surveillance images reveal that ZAMFIR visited this ATM two times between 4:54 AM and 6:04 AM. Images of ZAMFIR conducting these unauthorized withdrawals can be seen below:<sup>21</sup>



---

<sup>21</sup> ZAMFIR appears to be wearing a wig during these transactions.



Ionut ZAMFIR conducting unauthorized withdrawals at 244 Post Road WCCU ATM on 12/17/2023.

81. Video surveillance still images show Armando Ion CODREANU conducting unauthorized withdrawals at this same branch's drive through ATM from approximately 6:54 AM until approximately 7:04 AM. Although he is wearing a surgical-type mask while conducting these transactions, I believe this is Armando Ion CODREANU because he removes this mask exposing his face during a transaction at a Wakefield, RI WCCU ATM earlier this same morning. Several of the surveillance images from the Westerly ATM can be seen below:





Armando Ion CODREANU conducting unauthorized withdrawals at the 244 Post Road WCCU ATM on 12/17/2023.

82. On December 17, 2023, at approximately 4:31 am, WCCU video surveillance footage from the drive through ATM located at 64 Kingstown Road, Richmond RI location, captured Armando Ion CODREANU arrive in what appears to be a dark-colored vehicle while wearing a surgical mask. According to WCCU, this individual, whom I believe to be Armando Ion CODREANU, remained at the Richmond ATM from approximately 4:31 AM until approximately 5:27 AM conducting unauthorized withdrawals from WCCU customer accounts. In total, WCCU reported that there was \$54,100 withdrawn from seven victim accounts from approximately 4:33 AM through 5:15 AM. Below is a surveillance photo provided by WCCU of an individual I believe to be Armando Ion CODREANU at the Richmond ATM during this time:



83. According to WCCU, on December 17, 2023, from approximately 5:58 AM through 6:33 AM, video surveillance footage from the WCCU ATM located at 4979 Tower Hill Road in Wakefield, RI, captured an individual, whom I know to be Armando Ion CODREANU, at the drive-up ATM in what appears to be a dark colored vehicle. WCCU reported a total of \$30,000 in unauthorized withdrawals on December 17, 2023, from eight customer accounts at this Wakefield drive through ATM and an Interactive Teller Machine (ITM) onsite, from approximately 5:59 AM through 6:30 AM. WCCU only provided surveillance footage images from the Wakefield ATM during this time. One of these images shows Armando Ion CODREANU without a surgical mask covering his face. These images appear below:



84. It should be noted that one WCCU customer's account had unauthorized withdrawals from both the Dunns Corner (Westerly) and Wakefield branch ATMs on December 17, 2023. As described here, Armando Ion CODREANU was captured on this date at both locations conducting transactions at these ATMs.

85. December 17, 2023, WCCU reported unauthorized withdrawals totaling \$38,500 from nine separate WCCU accounts between approximately 5:19 AM and 6:11

AM at the branch located at 2405 Nooseneck Hill Road in Coventry, RI. These withdrawals occurred at both the Drive through and walk-up ATMs. On December 17, 2023, at approximately 5:18 am, video surveillance footage from the Coventry location, captured an unidentified male arrive to the drive through ATM in what appears to be a dark-colored sedan. WCCU reported that the unidentified male remained at this Coventry location from approximately 5:18 AM until 6:00 AM. A review of surveillance images of this unidentified male reveals that he appears to be the same individual who removed one of the skimming devices from the 122 Granite Avenue branch on December 15, 2023, as previously covered in this affidavit. Images of this unidentified male conducting transactions at the Coventry ATM during the time of these unauthorized transactions can be seen below:



86. WCCU reported \$34,500 in unauthorized withdrawals from eleven customer accounts from their drive through ATM located at their branch located at 122 Granite Street in Westerly, RI. These transactions took place between approximately 8:00 AM and 8:38 AM on December 17, 2023. No surveillance footage or images were

provided from these transactions.

87. WCCU also reported multiple unauthorized withdrawals from WCCU accounts that were conducted at ATMs belonging to two other regional banks on December 17, 2023. Three WCCU accounts were illegally accessed, and funds withdrawn using an unknown Berkshire Bank ATM. On this same date, beginning at approximately 7:30 AM, six WCCU accounts were illegally accessed, and a total of \$3,500 withdrawn using a Navigant Credit Union drive through ATM located in Westerly, RI. Navigant credit union provided surveillance footage from their Westerly drive through ATM during this time frame. I reviewed this surveillance footage and have determined that Armando Ion CODREANU conducts these unauthorized withdrawals. This footage shows Armando Ion CODREANU approach the Navigant ATM driving a dark-colored Toyota minivan. Although he is wearing a surgical-type face mask while conducting these transactions, I believe this is Armando Ion CODREANU because, as previously mentioned, WCCU provided a surveillance photo of him withdrawing funds from a Wakefield ATM earlier that day without the mask, while wearing a similar light-colored hooded sweatshirt. Furthermore, I am aware that Armando Ion CODREANU sometimes wears a cross earring that dangles from his left ear. A dangling cross earring can be seen on Armando Ion CODREANU's left ear below in the surveillance footage from the Navigant ATM on December 17, 2023, surveillance footage from Walmart in Warwick on December 16, 2023, as well as in his

California driver's license:<sup>22</sup>



88. This surveillance footage from Navigant shows that Armando Ion CODREANU is joined by another unidentified male in the front passenger seat of the vehicle. For approximately 13 minutes, the person I believe to be Armando Ion CODREANU, is the only person observed accessing the Navigant Credit Union ATM. During that time, Armando Ion CODREANU is observed to repeatedly insert gold-colored prepaid/gift type cards into the ATM, while manipulating the keypad and display screen. These cards do not appear to bear the Navigant logo and, based on what I have learned during this investigation, I believe that these cards used by Armando Ion CODREANU to conduct these transactions are cloned cards containing stolen banking data from WCCU customers whose information was compromised by the placement of the skimming devices on their Westerly ATMs. Armando Ion CODREANU is observed removing printed receipts and sums of currency from the

---

<sup>22</sup> It should be noted that the sweatshirt worn by Armando Ion CODREANU while at the Navigant ATM on December 17, 2023, appears to be the same or a similar sweatshirt that he wore the day before (December 16, 2023), when he joined Nicolas Longin CODREANU at the Walmart in Warwick, RI to install a skimming device at a self-checkout register. This sweatshirt has a grey-colored top, white on the lower half, and an unidentified emblem or writing on the left-hand side.



ATM throughout the duration of his visit to the Navigant ATM. During that timeframe, Armando Ion CODREANU is also observed manipulating a cellphone device. After conducting these transactions, Armando Ion CODREANU can be seen driving away from the ATM.

89. Based on these images, I believe that the deployment of skimming devices at the multiple BJ's and Walmart retail locations and the two financial institutions referenced herein, are related. The images from these incidents show that Nicolas Longin CODREANU and Armando Ion CODREANU worked together in the placement of skimming devices at several of the retail locations and were also both involved in the withdrawals of funds from compromised accounts at Bank Newport (Nicolas Longin CODREANU) and WCCU (Armando Ion CODREANU). And although Ionut ZAMFIR was not observed at the deployment of skimming devices at the retail locations, he was responsible for the deployment of ATM skimmers at Bank Newport and WCCU, along with Nicolas Longin CODREANU. ZAMFIR was also observed making fraudulent withdrawals at a WCCU ATM on the same date as Armando Ion CODREANU.

#### **Financial Account Analysis**

90. As part of this investigation, I sought financial records associated with the Target Subjects. I obtained records from Bank of America for Nicolas Longin CODREANU and Isabela Ignat CODREANU. According to Bank of America records, Nicolas Longin CODREANU opened a checking account (ending in 8544) in November of 2022 in Anaheim, CA. Isabela Ignat CODREANU opened a checking account (ending in 3779) in February of 2023 in Anaheim, CA.

91. A review of Nicolas Longin CODREANU's account reveals more than \$225,000 in deposits from January through December of 2023. Nicholas Longin CODREANU withdrew more than \$225,000 during that same time period. Most of the deposits into this account came from Zelle peer-to-peer transfers and ATM cash deposits. Most of the withdrawals were purchases, Zelle transfers, and ATM withdrawals.

92. A review of the Zelle deposits into and withdrawals out of Nicolas Longin CODREANU's account ending in 8544 reveals transfers among some of the co-conspirators. For example, in 2023, Nicolas Longin CODREANU sent and received 17 Zelle transfers to and from "MILA CIUCIU." Nicolas Longin CODREANU also had 49 Zelle transfers to and from "ISABELA CODREANU," and 32 transactions to and from I.P., the name of the individual believed to have been responsible for the placement of one of the skimming devices at a WCCU ATM on December 15, 2023.<sup>23</sup>

93. The cash deposits and withdrawals associated with Nicolas Longin CODREANU's checking account reveal frequent travel within the United States. Some of Nicolas Longin CODREANU's account activity from the account ending in 8544 reveals geographic patterns that coincide with instances where he and other co-conspirators were observed via surveillance footage engaged in the placement of skimming devices. For example, according to security photos from BJ's Wholesale Club, several skimming devices were placed by individuals matching the description of several of the Target Subjects in the New York City area on July 17, 2023. Nicholas Longin

---

<sup>23</sup> One of these transfers was in the form of an outgoing wire transfer.

CODREANU's checking account ending in 8544 shows debits from retail locations and Bank of America ATMs in the New York City area on this same date. Similarly, on July 17, 2023, an ATM withdrawal of \$40 was made at the Bank of America located in the Co-Op City section of Bronx, NY. A still image taken by Bank of America security footage at the time of this transaction on July 17, 2023, shows Robby Vicson CODREANU conducting this withdrawal from Nicolas Longin CODREANU's account while talking on his cell phone as seen below:



94. On this same date, BJ's reported that a skimmer was discovered on a register at their store located approximately 3 miles away from this ATM in Pelham, NY. Security photos show Nicolas Longin CODREANU, Armando Ion CODREANU, Robby Vicson CODREANU, Mila CIUCIU and others at this store on multiple dates in June and July of 2023, prior to the discovery of this device.

95. Another example of Nicolas Longin CODREANU's Bank of America showing account activity that coincides with his involvement in the placement of

skimming devices can be seen on July 17, 2023, in Linden, NJ. On this date, Nicolas Longin CODREANU's Bank of America account ending in 8544 recorded a purchase at a 7-Eleven store in Linden. On this same date, he could be seen at the BJ's in Linden with Mila CIUCIU. A skimming device was discovered at this store two days later on July 19, 2023. This 7-Eleven where he made a purchase is located approximately one mile from this BJ's Wholesale Club.

96. Nicolas Longin CODREANU's account also recorded transactions near the locations where he was suspected on deploying skimming devices in Rhode Island. For example, as previously stated herein, on October 18, 2023, Nicolas Longin CODREANU was observed via security footage deploying a skimming device on a Bank Newport ATM in Bristol, RI. Also on October 18, 2023, Nicolas Longin CODREANU's Bank of America account ending in 8544 recorded a \$1500 cash withdrawal at a Bank of America ATM located in East Providence, RI. Images of Nicolas Longin CODREANU conducting this withdrawal at the Bank of America located at 218 Taunton Avenue in East Providence can be seen below. It should be noted that Nicolas Longin CODREANU appears to be wearing the same or a similar t-shirt with unique lettering that he wore while installing a skimming device at the Bristol Bank Newport ATM machine on this same date.



Nicolas Longin CODREANU installing skimming device onto Bristol ATM on 10/18/2023.



Nicolas Longin CODREANU conducting personal ATM transaction in East Providence on 10/18/2023.

97. Further, on October 14<sup>th</sup> and 16<sup>th</sup> Nicolas Longin CODREANU's account posted Bank of America withdrawals at ATMs located in Westboro, MA and Marshfield, MA. I obtained surveillance footage from Bank of America of Nicolas Longin CODREANU conducting these transactions at Massachusetts Bank of America ATMs. It should be noted that in the surveillance images captured of Nicolas Longin CODREANU at the Bank of America on October 16, 2023, he appears to be wearing the same or similar grey Nike tracksuit that he wore when removing a skimming device from a Bank Newport ATM in Warren, RI.





Nicolas Longin CODREANU conducting an ATM transaction on  
10/14/2023 in Westborough, MA



Nicolas Longin CODREANU conducting an ATM transaction on  
10/16/2023 in Marshfield, MA

98. Based on this investigation, I am aware that Nicolas Longin CODREANU has provided a home address in Placentia, CA, and has no known ties to Rhode Island or

Massachusetts.

99. A review of Isabela Ignat CODREANU's account ending in 3779 reveals more than \$219,000 in deposits from February through December of 2023. Isabela Ignat CODREANU withdrew more than \$204,000 during that same time period. Most of the deposits into this account came from Zelle peer-to-peer transfers and ATM cash deposits. Most of the withdrawals were purchases and Zelle transfers.

100. A review of the Zelle deposits and withdrawals into and out of Isabela Ignat CODREANU's account ending in 3779 reveals transfers among some of the co-conspirators. For example, in 2023, Isabela Ignat CODREANU sent and received 7 Zelle transfers to and from "MILA CIUCIU" and 9 transfers to and from I.P. As previously stated herein, Isabela and Nicolas Longin CODREANU also had 49 Zelle transfers with each other.

101. Overall, the review of the accounts for both Nicolas Longin CODREANU and Isabela Ignat CODREANU show large cash deposits and withdrawals. For example, Nicolas Longin CODREANU's statement shows that from October 17, 2023, through November 14, 2023, he deposited more than \$8,000. I know from this investigation that Nicolas Longin CODREANU and Ionut ZAMFIR stole more than \$14,000 from Bank Newport customers on October 19, 2023. As previously stated herein, the theft of funds from Bank Newport customers was the result of CODREANU and ZAMFIR placing skimming devices on ATMs at several branches in Rhode Island. Isabela Ignat CODREANU also had frequent large cash deposits into her account ending in 3779. For example, her account statement covering November 22, 2023, through December 20, 2023,

shows \$11,500 in cash deposits, including seven deposits on December 20, 2023 alone totaling \$10,500. I believe that the frequent large cash deposits made into Nicholas and Isabela Ignat CODREANU's accounts represent cash that they illegally derived from card skimming incidents.

### **CONCLUSION**

Based on the information described above, I have probable cause to believe that from in or about May of 2023 through in or about April of 2024, in the District of Rhode Island and elsewhere, NICOLAS LONGIN CODREANU, IONUT ZAMFIR, ARMANDO ION CODREANU, ISABELA IGNAT CODREANU, MILA CIUCIU and ROBBY VICSON CODREANU knowingly conspired to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2), and NICOLAS LONGIN CODREANU, IONUT ZAMFIR, and ARMANDO ION CODREANU also conspired to commit bank fraud, in violation of 18 U.S.C. §§ 1344 and 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) and (c)(5).

Respectfully submitted,

  
Special Agent  
Homeland Security Investigations

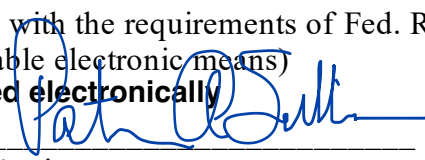
Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1. by: **Telephone** (specify reliable electronic means)  
**Sworn telephonically and signed electronically**

June 14, 2024

Date

**Providence, Rhode Island**

City and State

  
Judge's signature

Patricia A. Sullivan, U.S. Magistrate Judge  
Printed Name and Title