

Magistrate Judge Mary Alice Theiler

FILED ENTERED
LODGED RECEIVED

SEP 13 2011

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON DEPUTY
BY

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 ISMAIL SALI and)
 EUGEN TIRCA,)
)
 Defendants.)

CASE NO. **MJ11-434**
COMPLAINT for VIOLATION
Title 18, United States Code,
Section 1029(a)(4)

BEFORE the Honorable Mary Alice Theiler, United States Magistrate Judge, U.S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE
(Possession of Device-Making Equipment)

On or about June 18, 2011, at Bellevue, within the Western District of Washington, the defendants, ISMAIL SALI and EUGEN TIRCA, did knowingly and with intent to defraud, possess, produce, traffic in, have custody and control of, and aid and abet the production, trafficking, custody and control, and possession of, device-making equipment, specifically a pin hole camera and a card skimming device designed to be affixed to an Automated Teller Machine (ATM) at the US Bank Bellevue Highlands Branch in Bellevue, Washington, which conduct affected interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 1029(a)(4) and (c)(1)(A)(ii).

1 I, MALCOLM FREDERICK, being duly sworn on oath, depose and say:

2 **INTRODUCTION AND AGENT BACKGROUND**

3 1. I am a Special Agent with the United States Secret Service ("Secret Service") and
4 have been so employed since March 31, 2008. I am currently assigned to the Seattle Field
5 Office. I am a graduate of the Federal Law Enforcement Training Center located in Glynco,
6 Georgia. I am also a graduate of the Secret Service Special Agent Training Program located in
7 Beltsville, Maryland. Additionally, I am a graduate of the Washington State Basic Law
8 Enforcement Training Academy. Prior to my employment with the Secret Service, I was a
9 Commissioned Law Enforcement Officer with the Redmond Police Department for more than
10 fourteen years. I also have a Bachelor of Arts Degree from the University of Washington. In the
11 course of my official duties as a Special Agent with the Secret Service, I have been involved in
12 cases involving credit card fraud, bank fraud, access device fraud, and counterfeit currency and
13 securities. As part of my training with the Secret Service, I have received specialized instruction
14 on investigating financial crimes, credit card fraud, mail and wire fraud, identity theft, and the
15 manufacturing of counterfeit currency. I have also received specialized training in the
16 investigation of basic electronic crimes involving the use of computers and other electronic
17 devices.

18 2. This Affidavit is made in support of a complaint for the arrest of ISMAIL SALI
19 and EUGEN TIRCA, for violations of Title 18, United States Code, Section 1029(a) (Access
20 Device Fraud). The information contained in this Affidavit is based on my own personal
21 knowledge and information provided to me during my participation in this investigation,
22 including information provided by other law enforcement officers and witnesses. This Affidavit
23 is submitted solely for the purpose of establishing probable cause for the charge alleged in this
24 Complaint and does not purport to set forth all of my knowledge of, or investigation into, this
25 case.

26 **SUMMARY OF INVESTIGATION**

27 3. Since about June 2008, the Secret Service Electronic Crimes Task Force
28 ("ECTF"), Seattle Field Office, has been conducting investigations of credit/debit card skimming

1 activity, which has targeted Automated Teller Machines (“ATMs”) in Western Washington. The
2 ECTF is an investigative task force that is comprised of local law enforcement officers and
3 agents from the Secret Service. The investigation regarding ISMAIL SALI first was initiated by
4 Detective Donald Carroll of the Kirkland Police, who was developing evidence that SALI, along
5 with other suspects, were involved in the operation of a fraud scheme utilizing skimming devices
6 to compromise credit and debit cards used by the actual account holders to conduct legitimate
7 transactions. EUGEN TIRCA, a Romanian citizen believed to be illegally present in the United
8 States, is a known associate of SALI and a member of the fraud scheme. Secret Service ECTF
9 began encountering TIRCA in Fall 2010, but did not positively identify him until late
10 Spring 2011.

11 4. Based on this investigation, I have determined that ISMAIL SALI and EUGEN
12 TIRCA, and others have placed electronic skimming devices and video surveillance devices on
13 various ATMs and have used, without authorization, improperly obtained personally identifying
14 information of others, such as account data and PINs, to execute, or attempt to execute,
15 transactions at ATMs and various retailers, for the purpose of accessing funds to which they are
16 not entitled. The evidence establishing probable cause includes bank surveillance footage of
17 skimming activity and unauthorized transactions, surveillance footage from retailers of purchases
18 using cards encoded with victims’ account data; law enforcement surveillance; and information
19 provided by victims and witnesses.

20 **A. Background: Skimming and Skimming Devices**

21 5. Credit/debit card “skimming” is the theft of credit/debit card information used in
22 an otherwise legitimate transaction. Among other techniques, suspects often use manufactured
23 plastic materials that look similar to parts of the face plate of an ATM machine. Once this plastic
24 material is fabricated, an electronic card reader is placed inside the plastic. This small device
25 (the “skimmer” or “skimming device”) will store the information, or track data, of an
26 unsuspecting victim’s bank card. Suspects can place the plastic device over the actual ATM card
27 reader portal and intercept bank card information as the victim’s bank card is passed through the
28 device. In some instances where an ATM device is within a bank’s enclosed vestibule area,

1 suspects may place the skimming device inside or over card readers on the vestibule door. In
2 these instances, when a victim swipes their card through the vestibule card reader in order to
3 access the ATM after hours or on the weekend, the skimming device captures the card data.

4 6. In conjunction with these skimming devices, suspects will routinely install small
5 “pin-hole” cameras above or to the side of the ATM key pad. These cameras capture a victim’s
6 Personal Identification Number (“PIN”) as the customer uses the ATM machine. The times on
7 the skimming device are synchronized with the recorded times of the camera, which enables the
8 suspects to match a victim’s PIN with the information taken from the bank card. Often times
9 these cameras are installed using tape, glue, or other adhesive materials.

10 7. Skimming devices are often capable of holding data pertaining to hundreds or
11 even thousands of bank cards. Most skimming devices have an integrated USB port, which
12 allows data captured on the skimmer to be downloaded onto a laptop or desk top computer.
13 Suspects will typically retrieve their skimming devices, connect the skimming devices to a
14 computer, and then download the victim bank account data. Some devices contain wireless
15 transmission devices that allow the suspects to remotely retrieve data from the skimming device.
16 Typically, suspects will then transfer or “re-code” victim card data onto blank credit/debit card
17 stock, also known as white plastic. Suspects have also been known to re-code stolen card data
18 onto store gift cards. Any credit card sized plastic card with a magnetic stripe on the back of the
19 card may be used to re-code victim card data and access funds in the victim’s account. Given the
20 nature of the activity, skimming necessarily requires use of a computer and other digital devices,
21 including cameras, encoding equipment, and USB devices..

22 8. Once this process is complete, suspects use the newly made cards to access victim
23 bank account information at any available ATM machine or through point of sale purchases.
24 Typically, suspects will withdraw cash and also purchase consumer goods and merchandise
25 within a short period of time from the date that the debit card account was “skimmed.” In some
26 instances, however, suspects will wait several months before utilizing the stolen data. In either
27 case, however, suspects will typically conduct numerous fraudulent transactions in a short time
28 frame in order to maximize the use of the stolen data before the compromised bank or banks

1 recognize the breach and begin shutting down the compromised accounts.

2 **B. Evidence of Criminal Activity**

3 9. This investigation uncovered evidence supporting probable cause to believe that
4 ISMAIL SALI and EUGEN TIRCA have been involved in a criminal operation for some time,
5 and have committed various crimes, including access device fraud, in violation of Title 18,
6 United States Code, Section 1029(a). The following merely highlights supporting evidence.

7 **(1) 2010 ATM Skimming Activity**

8 10. On December 2, 2010, two suspects, I.A. and D.P., were arrested in Bothell,
9 Washington by local law enforcement officers after being observed engaging in suspicious
10 activity at multiple ATMs. The two suspects were driving a Jeep Cherokee. During a
11 subsequent warrant search of the Jeep, officers discovered more than 25 VISA debit cards
12 encoded with stolen bank customer data, a substantial amount of cash, and ATM and wire
13 receipts. Also recovered was mail addressed to ISMAIL SALI and a 2008 title certificate
14 showing SALI as the legal owner of the vehicle (or at least a past legal owner). The Jeep
15 Cherokee is currently registered to a known female associate of SALI, whose initials are N.B., at
16 an apartment in Redmond, Washington, as are other vehicles associated with SALI and TIRCA.
17 I.A. and D.P. used this Redmond address on their Washington State identification cards.

18 11. Both I.A. and D.P., who, like EUGEN TIRCA, are Romanian citizens unlawfully
19 present in the United States, were charged federally based on their alleged involvement in
20 numerous skims of ATMs and unauthorized withdrawals from hundreds of victims' accounts. A
21 third unidentified male suspect is seen repeatedly in bank surveillance video with I.A. and D.P.
22 both placing devices on ATMs and executing fraudulent ATM withdrawals. That third suspect
23 was thereafter identified as EUGEN TIRCA based on known photographs and images, including
24 TIRCA's Washington Department of Licensing photograph. An ATM surveillance image of
25 D.P. and TIRCA together during a skimming incident is attached as **Exhibit A**.

26 12. Several vehicles were associated with the skimming activity committed with I.A.,
27 D.P., and TIRCA. In addition to the Jeep Cherokee driven on the day of I.A.'s and D.P.'s arrest,
28 a black Mercedes SUV and a white full-size van are plainly visible on surveillance video in

1 connection with known skimming incidents. All of these vehicles are associated with the known
2 residence of SALI, which is located in Kirkland, Washington (hereafter, "SUBJECT
3 PREMISES"). Surveillance has further confirmed that TIRCA also resides at this SUBJECT
4 PREMISES, and that SALI and TIRCA are primary users of the aforementioned vehicles.

5 a. As one example, on November 1, 2010, unauthorized cash withdrawals,
6 and additional attempts, were made at a Boeing Employees' Credit Union ("BECU") ATM in the
7 Lower Queen Anne neighborhood in Seattle. I also have reviewed the ATM surveillance video,
8 which shows that at approximately 4:14 p.m., a white full-size van stops directly in front of the
9 ATM. The driver of the white van is not visible. A male suspect, plainly identifiable as I.A.,
10 exits the passenger-side door, approaches the ATM, and executes several sequential ATM
11 transactions using various cards. He then returns to the passenger seat in the van. Then, at about
12 4:17 p.m., a second suspect, readily identifiable as D.P., exits the back-seat sliding door of the
13 van, approaches the ATM, and makes several transactions. At times, D.P. covers the camera
14 with his hand. D.P. returns to the van, entering the back sliding door, and, at approximately 4:19
15 p.m., the van drives away. From reviewing the transaction data, I know that the victimized
16 accounts were compromised through prior skimming incidents at other BECU ATM locations.

17 b. As another example, a BECU ATM located on Coal Creek Parkway, in
18 Newcastle, Washington was skimmed on October 15, 2010. I have reviewed ATM surveillance
19 images from this skimming incident, which shows a white full-size van in front of the ATM at
20 around 10:56 a.m. D.P. then appears to affix the skimming device onto the ATM. Then, at
21 about 1:47 p.m., a black Mercedes SUV stops in front of the ATM. I.A. and D.P. are visible on
22 surveillance footage and appear to remove devices from the ATM. Sample surveillance images
23 are attached as **Exhibit B**.

24 13. Both I.A. and D.P. have entered pleas of guilty to several criminal counts arising
25 from their skimming activity and unauthorized ATM withdrawals from victim accounts. Both
26 defendants currently await sentencing.

1 (2) **March 3, 2011 Surveillance.**

2 14. On March 3, 2011, detectives with the Bellevue Police Department (“BPD”) and
3 agents with the Secret Service conducted a surveillance operation on the SUBJECT PREMISES.
4 The purpose of this surveillance was to identify additional suspects and collect additional
5 evidence in furtherance of the ongoing investigation into ATM skimming activity. Three
6 vehicles associated with this residence, namely, (1) a black 1999 Mercedes ML430, (2) a white
7 1997 Chevrolet G3 van, and (3) a 1989 Ford F150 truck, as well as others, were present at the
8 beginning of this surveillance operation.

9 15. At approximately 4:30 p.m., surveillance witnessed a male subject drive the Ford
10 truck out of the driveway of the residence and park it in the cul-de-sac. This subject then got into
11 the white van, which was parked in front of the residence, and drive away. This subject was
12 wearing a light-colored hat, dark-colored jacket (possible black or dark grey), and blue jeans.
13 The subject had the jacket zipped up all the way to his neck.

14 16. Investigators followed the van as it left the residence. A short time later
15 surveillance was lost. At approximately 4:40 p.m., BPD Detective Shelby Shearer located the
16 van in a 7-11 parking lot, at 13335 100th Ave NE, in Kirkland. Detective Shearer then contacted
17 the employee at 7-11 and confirmed that the driver of the van had been inside the store and made
18 a cash purchase.

19 17. On this same day, at approximately 4:48 p.m., Detective Herst and Detective
20 Shearer followed the van as it drove into the parking lot of a Safeway store, also in Kirkland.
21 The driver (and the lone occupant of the vehicle) parked the van and walked into the store.
22 Detective Herst looked into the van through the driver's window and observed what appeared to
23 be one or more credit/debit cards sitting upside down on the middle console.

24 18. Detective Herst then walked into the Safeway, located the driver and followed
25 him as he shopped inside the store. The suspect matched the description of ISMAIL SALI. The
26 man, believed to be SALI, purchased \$209.37 in groceries. Detective Herst was standing in line
27 behind this subject as he attempted to pay using a card, which was immediately declined. The
28 man then presented another credit card, which was accepted. The man also used a Safeway Club

1 Card to compliment his purchase.

2 19. Once this purchase was complete, the subject walked outside, loaded his groceries
3 into the van, and then drove out of the parking lot. Surveillance followed the van as it drove
4 directly from the Safeway store back to the SUBJECT PREMISES, arriving at approximately
5 5:30 p.m. There, investigators witnessed the man and a second unknown individual unload the
6 groceries from the van and carry them into the residence.

7 20. Detective Herst later contacted Safeway Fraud Investigator Ingrid Bechtel
8 regarding the suspect's \$209.37 purchase that had taken place at Safeway. Bechtel provided
9 Detective Herst with the credit card information that had been used to complete the grocery
10 purchase. A Bank of America VISA credit card, account number ending in -8508, was used first
11 and had been declined. An American Express ("AMEX") credit card, account number ending in
12 -1005, was used to complete the grocery purchase.

13 21. I have confirmed that neither the VISA nor AMEX account belongs to SALI. The
14 owner of AMEX credit card (no. -1005), whose initials are P.K., reported that she did not make
15 nor authorize the grocery purchase at Safeway and that she still had the credit card in her
16 possession. P.K. also told investigators that she had multiple fraudulent charges on her credit
17 card account, including an unauthorized purchase of \$288.58 at an Albertson's store, at 9826 NE
18 132nd Street, Kirkland, Washington, on March 4, 2011. Investigators obtained and reviewed
19 Albertson's surveillance video associated with this fraudulent transaction using P.K.'s account
20 data. The video depicts a male and a female, along with a small child, purchasing groceries. The
21 male, who paid for the groceries using a card, matches the description and appears to me to be
22 ISMAIL SALI. I also recognize the female and child, who are known associates of SALI.

23 22. The owner of VISA credit card (no. -8508) is a person with initials of X.J.
24 According to Bank of America Investigator Paul Lemon, this credit card account had been closed
25 due to reported fraudulent activity. Lemon provided investigators with additional fraudulent
26 transaction information, which included two attempted payments at King County Solid Waste
27 Station #20 on March 2 and 4, 2011. Investigators contacted King County Solid Waste and
28 obtained video surveillance footage of both these attempted transactions. Investigators reviewed

1 this video, which consisted of several different camera angles, to include the ingress and egress
2 from the payment station area. This video clearly shows the same vehicle, namely, a white
3 full-size van with no side windows, at the payment station at the time at which X.J.'s VISA card
4 was being used on March 2 and 4, 2011. The front bumper of the van, which does not have a
5 front license plate, is very distinctive, as it has a large dent, with visible rusted edges, located just
6 to the right of center. I recognize this van as the same van that consistently is parked in front of
7 the SUBJECT PREMISES, that SALI and TIRCA regularly drive, and that was driven as part of
8 the March 3, 2011, fraudulent transactions.

9 *(3) March 19, 2011 Skimming Incident*

10 23. US Bank identified a skimming incident that occurred on March 19, 2011, at the
11 US Bank Juanita Branch ATM, located at 13233 100th Ave NE Kirkland, Washington 98034. In
12 total, approximately 24 individuals had their account data skimmed during this incident.
13 Beginning the following day, March 20, 2011, and continuing for the following few days,
14 numerous transactions were attempted using the account data of the aforementioned skimming
15 victims. Based on my training and experience regarding skimming operations, I know that this
16 means that the suspects synchronized the skimmed account data and video of PIN information,
17 encoded skimmed account data onto blank card stock, and manufactured counterfeit cards, all of
18 which requires the use of digital devices, including computers, almost immediately after the
19 skimming incident occurred.

20 24. US Bank ATM surveillance video from March 19, 2011, shows a male suspect
21 placing a device on the ATM at 3:18 p.m. and a second male suspect later returning to remove
22 the device at about 6:27 p.m. US Bank Investigator David Hauth has confirmed that no
23 legitimate electronic transaction occurred while either of the suspects were standing at the ATM.
24 The first suspect is seen approaching the ATM and clearly removes a long narrow device from
25 inside his jacket, which he then installs on the ATM. Approximately three hours later, the
26 second suspect, wearing a hat and sunglasses in an effort to conceal his identity, is seen standing
27 in front of the ATM for approximately thirty seconds, as, it appears, he removes a skimming
28 device from the ATM. Sample surveillance images are attached as **Exhibit C**.

1 25. Based on my review of the surveillance video, other images of known persons,
2 including Washington Department of Licensing photographs, I believe that EUGEN TIRCA is
3 the individual installing the skimming device and ISMAIL SALI is the individual later removing
4 the device.

5 (4) *June 18, 2011 Skimming Activity*

6 26. Another skimming incident occurred on June 18, 2011, at the US Bank Bellevue
7 Highlands Branch ATM, located at 13830 NE 20th Street, Bellevue, Washington 98005. A
8 skimming device was placed on this ATM between about 3:24 and 4:41 p.m. During this period,
9 at least six victims used this ATM and had their accounts compromised. Over the following
10 days, approximately 45 unauthorized transactions were attempted using these victims' accounts
11 in a total attempted amount of over \$18,000.

12 27. The US Bank Investigator David Hauth provided ATM surveillance video of the
13 June 18, 2011, incident. A white full-size van, which appears to be the van associated with
14 SALI, TIRCA, and the SUBJECT PREMISES, pulls into one of two handicapped parking stalls
15 located in front of the bank branch. (In prior surveillance, I have observed a handicapped placard
16 hanging from the rear-view mirror of SALI's van.) A male suspect, wearing a light-colored hat
17 and a dark vest over a hooded sweatshirt, appears to exit the passenger side of the van and
18 approach the ATM. The suspect, whom I believe to be EUGEN TIRCA, then removes long
19 narrow device, i.e., what appears to be a skimming device, from his jacket and appears to affix it
20 to the ATM at about 3:24 p.m. The suspect departs the ATM and returns toward the van when a
21 legitimate customer approaches. A second male suspect, wearing a dark long-sleeve coat, blue
22 jeans, and a dark baseball cap, is visible loitering in the background. As the legitimate customer
23 departs, the second suspect, whom I believe to be ISMAIL SALI, approaches the ATM and
24 appears to tinker with and perhaps test the skimming device. The second suspect then leaves the
25 ATM, enters the driver's door of the white van, and drives the van from the scene.

26 28. Approximately ninety minutes later, at about 4:41 p.m., the first suspect, whom I
27 believe to be EUGEN TIRCA, returns to the ATM and removes the device. Hauth has confirmed
28 that no legitimate electronic transaction occurred while the suspect was standing at the ATM on

1 either instance.

2 29. On June 18, 2011, the SUBJECT PREMISES was under surveillance by members
3 of Secret Service ECTF. Over the course of the day, EUGEN TIRCA and ISMAIL SALI are
4 seen entering and exiting the residence and leaving and returning to the SUBJECT PREMISES.
5 Specifically, on this date at approximately 2:06 p.m., TIRCA and SALI exit the residence, get
6 into the white van, and depart. TIRCA is wearing a gray, long-sleeve hooded sweatshirt, a dark
7 (possibly black) vest, and a light-colored baseball cap with writing on the front. SALI is
8 wearing a dark long-sleeve coat, blue jeans, and a dark baseball cap. At approximately 5:04
9 p.m., the white van returns to the SUBJECT PREMISES. TIRCA and SALI, wearing the same
10 clothing as before, exit the vehicle and walk into the residence.

11 **(5) June 19, 2011 Unauthorized Withdrawals**

12 30. On June 19, 2011, surveillance on the SUBJECT PREMISES continued. At
13 approximately 5:14 p.m., TIRCA and SALI leave the SUBJECT PREMISES in the white van.
14 TIRCA is wearing a shiny dark-colored (perhaps purple) long-sleeved jacket, a light blue shirt,
15 and a beige colored baseball cap with a symbol on the front.

16 31. On June 19, 2011, between about 5:25 and 5:35 p.m., there were about seven
17 unauthorized cash withdrawals and ten additional attempted unauthorized cash withdrawals at
18 the US Bank ATM located at 6460 Bothell Way, in Kenmore, Washington. This ATM location
19 is less than four miles and an estimated 10-minute drive from the SUBJECT PREMISES.
20 According to Hauth, all of the successful and attempted unauthorized cash withdrawals were
21 made on victim accounts that had been compromised during the skimming incident at the US
22 Bank Bellevue Highlands Branch on the prior day, June 18, 2011, discussed above. A review of
23 bank surveillance video shows that the same suspect, whom I believe to be EUGEN TIRCA,
24 conducts each of the fraudulent transactions. In each of these transactions the male suspect is
25 wearing a shiny dark-colored long-sleeved jacket, a light blue shirt, and a beige colored baseball
26 cap.

27 32. At approximately 6:21 p.m., the white van returns to the SUBJECT PREMISES,
28 and TIRCA and SALI exit the vehicle and walk into the residence.

1 37. Investigation into the details surrounding the purchase of the above-mentioned
2 items has revealed that SALI fraudulently purchased these items from a Safeway grocery store in
3 downtown Bellevue, Washington, using the account data of several fraud victims. Safeway
4 video surveillance captured images of SALI as he is making the fraudulent purchase. More
5 specifically, on August 17, 2011, at approximately 1:40 p.m., SALI attempted to use Alaska USA
6 Federal Credit Union debit card number ending in -2044; which belongs to account holder B.H.,
7 for the \$283.28 purchase. This card was immediately declined. SALI then attempted to
8 complete this purchase with a second debit card. The second card, encoded with a Capital One
9 debit card number ending in -2612, which belongs to account holder S.K., was also declined.
10 SALI then used a third card, encoded with Citi Bank debit card number ending in -1131,
11 belonging to L.C., which was approved.

12 38. Investigators contacted Alaska USA, Capital One, and Citi Bank regarding the
13 August 17, 2011, grocery purchase. Alaska USA confirmed that debit card number ending in
14 -2044 belonged to account holder B.H. and that the card had been cancelled on August 16, 2011,
15 due to suspicious activity originally reported on August 12, 2011. Investigators spoke with B.H.,
16 who confirmed he had not attempted nor authorized the purchase at Safeway. Capital One
17 confirmed debit card number ending in -2612 belonged to S.K. and had experienced multiple
18 fraudulent attempted purchases in the week before August 17, 2011. Investigators spoke to S.K.,
19 who confirmed he had not attempted to make nor authorized the purchase at Safeway. Citi Bank
20 confirmed that debit card number ending in -1131 was issued to L.C., the card was still active,
21 and no fraud had been reported. Investigators then contacted L.C., who confirmed that neither he
22 nor any of the authorized users of the card had made a purchase at Safeway in Bellevue on
23 August 17, 2011.

24 39. Based on my training and experience and on this investigation, I believe that
25 ISMAIL SALI and EUGEN TIRCA have used "device-making equipment" to obtain victim
26 information and "unauthorized access devices" and "counterfeit access devices" to execute
27 unauthorized and fraudulent transactions. Title 18, United States Code, Section 1029(e), defines
28 these terms as follows:

1 a. the term "access device" means any card, plate, code, account number,
2 electronic serial number, mobile identification number, personal identification number, or other
3 telecommunications service, equipment, or instrument identifier, or other means of account
4 access that can be used, alone or in conjunction with another access device, to obtain money,
5 goods, services, or any other thing of value, or that can be used to initiate a transfer of funds
6 (other than a transfer originated solely by paper instrument);

7 b. the term "counterfeit access device" means any access device that is
8 counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a
9 counterfeit access device;

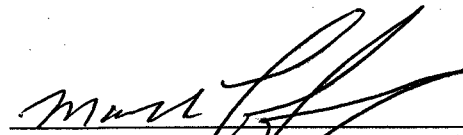
10 c. the term "unauthorized access device" means any access device that is
11 lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

12 d. the term "device-making equipment" means any equipment, mechanism,
13 or impression designed or primarily used for making an access device or a counterfeit access
14 device.

15 40. I know, based on my training and experience, that each of the banks and credit
16 unions discussed above are financial institutions, as defined in Title 18, United States Code,
17 Section 20, because they are either insured by the Federal Deposit Insurance Corporation or the
18 National Credit Union Share Insurance Fund.

19 **CONCLUSION**

20 9. Based on the above facts, I respectfully submit that there is probable cause to
21 believe that ISMAIL SALI and EUGEN TIRCA did knowingly and intentionally commit the
22 crime of access device fraud, in violation of Title 18, United States Code, Section 1029(a)(4),
23 among other crimes.

24
25 
26 MALCOLM FREDERICK, Complainant
27 Special Agent, U.S. Secret Service
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendants committed the offense set forth in the Complaint.

Dated this 13 day of September, 2011.



HON. MARY ALICE THEILER
United States Magistrate Judge

EXHIBIT A



21045 Bothe II - Everett Hwy.
09/06/2010

09/25/2010 17:59:32.24

EXHIBIT B



6920 Coal Creek Parkway SE 10/15/2010 10:58:32.63



6920 Coal Creek Parkway SE 10/15/2010 13:47:10.69
ATM 900



6920 Coal Creek Parkway SE 10/15/2010 13:48:06.82
ATM 900

EXHIBIT C

Digital Video Snapshot

Site: Pacific Division/Northwest Region/WA/8240 Juanita

Camera Group: 8240 Juanita

Camera Name: 02 ATM 2

3/19/2011 3:18:03 PM (Pacific Daylight Time)



Capture Size: 352 x 240 pixels

Device Network Name: PSVWA16HL01M01

Device Serial Number: GS0825E126

Device Station ID: 8240 Juanita

Digital Video Snapshot

Site: Pacific Division/Northwest Region/WA/8240 Juanita

Camera Group: 8240 Juanita

Camera Name: 02 ATM 2

3/19/2011 6:22:52 PM (Pacific Daylight Time)



Capture Size: 352 x 240 pixels

Device Network Name: PSWV-18-L01101

Device Serial Number: GS0825E128

Device Station ID: 8240 Juanita