UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | Hon. Madeline Cox Arleo |
| v. | : | Mag. No. 11-8153 (MCA) |
| RAZIA BIBI and<br>TAHIR LODHI | : | **CRIMINAL COMPLAINT** |

I, James Simpson, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

James Simpson, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
August 30, 2011 at Newark, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

From in or about November 2006 through the present, in the District of New Jersey, and elsewhere, defendants

RAZIA BIBI and
TAHIR LODHI

did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud financial institutions, and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, those financial institutions, by means of false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344 and Section 2.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, James Simpson, a Special Agent with the Federal Bureau of Investigation ("FBI"), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause:

**Background**

1. At all times relevant to this complaint:

a. Credit cards were issued by banks and other financial institutions (the "Card Issuers"), and allowed consumers to obtain goods and services with the understanding that the consumers would repay the Card Issuers pursuant to contractual agreements between the consumers and the Card Issuers.

b. Credit report companies, including "Credit Report Company A," provided information to subscribers relating to the credit scores of applicants for, and recipients of, credit cards.

c. The majority of credit cards were applied for online. To apply for a credit card online, a consumer accessed the website of a Card Issuer, and completed an application form.

d. Unbeknownst to the person applying for the card, however, many Card Issuers installed tiny pieces of computer code, known informally as "cookies," onto the applicant's computer. These cookies were used to send information to the applicant's browser and for the browser to return information to the origin site; here, the site of the Card Issuer.

e. Much useful information could be derived from cookies: they could be used for authentication, identification of a user session, automatic setting of a user's preferences, retention of shopping cart contents, storage of passwords, or anything else that could be accomplished through storing text data.

f. Card Issuers used certain cookies to identify the specific machine that had created a credit card application, and to track how many applications that specific machine had created in total. In other words, the Card Issuers used cookies to "tag" a specific computer with a "Device ID." Thus, each time a specific machine applied for a credit card, the cookie could track whether that device had applied for a card before, and how many times.

g. The Card Issuers stored information derived from cookies.

h. A credit card "bust out" scheme involved several steps. First, the conspirators applied for credit card accounts in the names of third parties, who were often fictitious identities created by the conspirators. Second, the conspirators directed credit cards obtained by fraud to addresses they controlled. Third, the conspirators raised the credit limit on these credit cards. This was accomplished in two ways: they either made numerous small transactions at different businesses, and then paid the balances on a

timely basis; or they made fraudulent payments toward the balances on the cards by paying the balances using bank accounts that, while real, had insufficient funds to cover the payments. Fourth, once the credit limits were sufficiently high, the conspirators "busted out" the credit cards by charging large amounts on the credit cards and failing to pay off the balances.

**The Fraudulent Scheme**

2. The FBI is investigating a large-scale conspiracy to obtain Fraudulent Cards, build the credit limit of these cards, and then "bust out" the Fraudulent Cards. The Fraudulent Cards are busted out by making large purchases at complicit merchants, by writing convenience checks on the Fraudulent Cards' accounts, or by taking large cash advances using the Fraudulent Cards. Because none of the large charges, checks, or advances are ever paid back, the Card Issuers suffer losses on the Fraudulent Cards.

3. From in or about November 2006 to the present, defendants RAZIA BIBI and TAHIR LODHI, and others, conspired to commit a credit card bust out scheme by opening or accessing approximately 3,390 credit cards in the names of over 600 fictitious or otherwise fraudulent identities (collectively, the "Fraudulent Cards"), collecting mail relating to Fraudulent Cards, running credit reports for Fraudulent Cards from addresses they controlled, and then busting out Fraudulent Cards. The total losses caused by the fraud scheme exceed $10 million.

4. The investigation focused first on two individuals, Cooperating Defendant 1 ("CD-1") and Cooperating Defendant 2 ("CD-2"), who were building up credit on fraudulent credit cards through gas stations and cell phone stores in New Jersey run by CD-1 and CD-2. Once the credit limits on these cards had been extended or additional credit freed up, CD-1 and CD-2 busted out these cards. As a result of the bust-out scheme perpetrated by CD-1 and CD-2, approximately 12 Card Issuers and banks lost approximately $823,000.

5. CD-1 and CD-2 were arrested in or around August 2010. As part of CD-1's cooperation with law enforcement, CD-1 provided information about three jewelry stores in and around Jersey City, New Jersey, which CD-1 believed were processing large numbers of transactions from fraudulently-obtained credit cards (the "Jersey City Jewelers"). The investigation turned towards the Jersey City Jewelers and their owners. Based on my practice and experience, I know that because large transactions are common at jewelry stores, they are ideal vehicles for carrying out credit card "bust out" fraud schemes.

6. Through investigation of the Jersey City Jewelers, law enforcement officers developed probable cause to believe that the Jersey City Jewelers were being used to run hundreds of fraudulently obtained credit cards in the names of fictitious persons. After the cards were run, the credit card companies and merchant processors, believing that legitimate transactions had taken place, made payment to the Jersey City Jewelers, while the fictitious persons, of course, never made payments toward the balances due and owing.

7. In or around April 2011, search warrants were executed at the Jersey City Jewelers, and over $2 million in gold jewelry was seized as being connected with the credit card bust out scheme under investigation.

**The Chaudry Fraud Cards – An Example**

8. As explained above, defendants perpetrated their fraud by using fictitious identities. One fictitious identity created by the conspirators in or about 2008 was "Mona Chaudry." Between in or about January 2008 and in or about May 2011 this identity was used to generate approximately 11 Fraudulent Cards (collectively, the "Chaudry Fraud Cards"). Five of these cards were busted out. The total loss to credit card issuers from the five busted out Chaudry Fraud Cards is approximately $30,124.

9. One of the Chaudry Fraud Cards was a Bank of America card in the name of Mona Chaudry ending with '6021 (the "'6021 Chaudry Fraud Card").

10. The '6021 Chaudry Fraud Card has been connected to several locations linked to the conspirators.

11. For example, on or about March 7, 2011, the credit report for the '6021 Chaudry Fraud Card was accessed from both:

a. Computers associated with 960 South Broadway, Suite 107, Hicksville, New York, which is defendant LODHI's place of business ("Defendant LOHDI's Business"); and

b. Computers associated with 356 Ridge Road, Apartment A-12, Dayton, New Jersey, which is defendant BIBI's residence ("Defendant BIBI's Residence").

12. Just a couple weeks later, as part of the conspiracy, defendants began busting out the '6021 Chaudry Fraud Card:

a. On or about March 25, 2011, the '6021 Chaudry Fraud Card was used to make a charge of approximately $4,975.00 at a jewelry store named Ashu Jewels, one of the Jersey City Jewelers. None of this money has been paid back.

b. Then, on or about April 14, 2011, a cash advance of approximately $4,965 was taken out on the '6021 Chaudry Fraud Card. None of this money, either, has been paid back.

c. The '6021 Chaudry Fraud Card is currently in default.

13. Law enforcement officers have recovered the security tapes from Ashu's security system, which demonstrate that the March 25, 2011 bust out transaction on the '6021 Chaudry Fraud Card was, indeed, a product of the conspiracy.

14. The tape shows that at or around 4:30 p.m., defendant BIBI entered Ashu Jewels. Sat Verma ("Sat"), the owner of Ashu Jewels, was in the store, along with his wife, Sharn Verma ("Sharn"). One other customer was in the store. Defendant BIBI and the Vermas waited for the customer to leave Ashu Jewels. After the customer left, defendant BIBI and the Vermas were alone in the store. At no time did defendant BIBI try on any jewelry; at no time did the Vermas even show defendant BIBI any jewelry.

15. Instead, Defendant BIBI simply pulled two credit cards out of her handbag and handed them to Sharn. Sharn took the cards to the merchant terminal, located in the back of the store. Shortly thereafter, Sharn returned to the counter area, where Sharn, Sat, and defendant BIBI stood as Sharn filled out a fake and fraudulent receipt for phantom

"jewelry" that was being purchased on the '6021 Chaudry Fraud Card. (The other card apparently was denied when Sharn attempted to run it.)

16. After a short period, defendant BIBI took the two cards, including the '6021 Chaudry Fraud Card, back from Sharn, and exited Ashu Jewels – without any jewelry.

17. Law enforcement officers have obtained receipt books from Ashu Jewels. Those books contain copies of both the Ashu Jewels receipts and the merchant's copy of the credit card receipts for transactions that took place at Ashu Jewels.

18. Within the receipt book was a merchant's receipt that matched precisely the date and time of the video tape.[1] The receipts reflected that at that date and time, the '6021 Chaudry Fraud Card was used to make a $4,975.00 purchase of jewelry, and the merchant's receipt was signed "Mona Chaudry." The video tape, of course, revealed that no one named Mona Chaudry was in the store at that date and time, and that the transaction was part of the conspiracy.

**The Safdar Fraud Card – An Example**

19. On or around October 10, 2008, someone applied for a credit card with Hudson Valley Federal Credit Union ending in 5975 in the name of "Mohammad Safdar" with an address of 4501 Twin Oaks Court, Monmouth Junction, New Jersey 08852 (the "Safdar Fraud Card"). Based on a review of law enforcement and other databases, there is probable cause to believe that Mohammad Safdar is a fictitious person.

20. After the Safdar Fraud Card was issued, it was used to make thousands of dollars of "purchases" at Ashu Jewels and Tanishq Jewelers (another of the Jersey City Jewelers) as follows:

| Date | Amount | Store |
|---|---|---|
| October 26, 2008 | $4,850 | Ashu Jewelers |
| October 29, 2008 | $4,442 | Tanishq Jewelers |

21. Although Hudson Valley Federal Credit Union paid those amounts to the two jewelry stores, no monies were ever paid by Mohammad Safdar, or anyone else, to Hudson Valley Federal Credit Union.[2]

---

[1] More specifically, the date was exactly the same, and the time stamp from the security camera was exactly one hour behind, indicating that the security camera was set to Central Standard Time. When law enforcement officers shut down the tape during the search of Ashu Jewels they made note of the Eastern Standard Time of the shut down, and compared it to the time stamp displayed on the security tape. The tape was exactly one hour behind.

[2] The fictitious identity of "Mohammad Safder" is connected to defendant BIBI in yet another way. During surveillance conducted at defendant BIBI's residence in or around July 2011, law enforcement officers observed a black 2007 Toyota Land Cruiser, registered to "Mohammad Safder" (the "Safder Land Cruiser"). In or around 2008, defendant BIBI filed a police report with the Jersey City police claiming that her vehicle had been broken into – a black 2007 Toyota Land Cruiser with the same license plate as the Safder Land Cruiser. Accordingly, there is

22. Defendant BIBI leased the location at 4501 Twin Oaks Court (the "4501 Twin Oaks Address") under the name "Riaze Bibe," and paid the rent on the 4501 Twin Oaks Address using postal money orders drawn on a Bank of America account in the name of "Razia Bibi" (the "Defendant BIBI Bank Account").

23. Defendant BIBI has also used postal money orders drawn on the Defendant BIBI Bank Account to pay the rent on at least 9 other addresses, each of which received mail connected to Fraudulent Cards.

24. A review of hundreds of Fraudulent Cards revealed that a total of approximately 62 were associated with the 4501 Twin Oaks Address.

25. Of the 62 cards associated with the 4501 Twin Oaks Address, 15 – including the Safder Fraud Card – were created from a single Internet Protocol ("IP") address.[3]

26. This IP address resolved to 407 Abbi Road, Cartaret, New Jersey (the "Abbi Road IP Address"). At the time these 15 cards were applied for from the Abbi Road IP Address, defendant BIBI was living at 411 Abbi Road in Cartaret. 411 Abbi Road is directly downstairs from 407 Abbi Road.

27. In total, approximately 95 Fraudulent Cards were applied for from the Abbi Road IP Address (including, of course, approximately 80 Fraudulent Cards that did not use the 4501 Twin Oaks Address).

28. For example, five of the 95 Fraudulent Cards used an address of 6405 Shadow Oaks Court, Monmouth Junction, New Jersey (the "6405 Shadow Address").

29. In or around July 2009, co-conspirator 1 ("CC-1") was interviewed by law enforcement authorities. At the time of the interview, CC-1 had approximately 59 keys on his person. One of the keys was labeled "6405 Shadow." Subsequently, CC-1 stated, in sum and substance, that:

a. his job was to collect mail from the locations that matched the keys and take the mail to locations in New York;

b. he received money for this work; and

c. part of CC-1's "mail route" was to pick up mail at the 6405 Shadow Address.

30. Defendant BIBI paid the rent at for the 6405 Shadow Address using postal money orders drawn on a bank account in her name.

**The Shah Fraud Card – An Example**

31. Investigation has revealed that on or around May 21, 2011, someone applied for a credit

---

probable cause to believe that defendant BIBI actually controls the Safder Land Cruiser.

[3] Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access a particular website or account.

card with USAA ending in 5647 in the name of "Tahir Shah" (the "Shah Fraud Card"). This application was made from a IP address that resolved back to 4 Mercury Place, Hicksville, New York, an address where defendant LODHI has been surveilled residing ("Defendant LODHI's Residence").

32. Based on a review of law enforcement and other databases, there is probable cause to believe that Tahir Shah is a fictitious person. A review of several hundred of the Fraudulent Cards revealed that approximately ten were associated with the same address as that used for the Shah Fraud Card.

33. After the Shah Fraud Card was issued, the Card Issuer sent "Convenience Checks" to the address associated with the Shah Fraud Card, as part of the normal correspondence that a Card Issuer sends to a card subscriber. The user of the Shah Fraud Card, however, used these Convenience Checks to draw thousands of dollars from the Shah Fraud Card Account, as follows:

| Date | Amount |
|---|---|
| May 27, 2011 | $3,900 |
| June 14, 2011 | $4,300 |
| July 11, 2011 | $2,000 |

34. Although USAA paid those amounts for the convenience checks, no monies were ever paid by Tahir Shah, or anyone else, to USAA, since, as noted above, Tahir Shah is believed to be a fictitious person.

35. The Shah Fraud Card is tied to defendant LODHI. Specifically, and besides the login on or about May 21, 2011, the Shah Fraud Card was also logged into from Defendant LODHI's Residence on or about May 24, 2011 and on or about May 26, 2011. These logins to the Shah Fraud Card took place immediately prior to the beginning of the bust out of the Shah Fraud Card Account.

36. The Shah Fraud Card was also logged into from at or around 960 South Broadway, Suite 107, Hicksville, New York, where defendant LODHI is believed to work ("Defendant LODHI's Business"). Specifically, the Shah Fraud Card was logged into from an IP address that resolved to Defendant LODHI's Business on or around on or about June 30, 2011, July 8, 2011, July 11, 2011, and July 12, 2011. Again, these login dates were immediately surrounding the dates of the bust out of the Shah Fraud Card.

37. As part of the conspiracy, the defendants used the Shah Fraud Card to pay for an account with Credit Report Company A ("the Credit Report Company Account"). Such an account can assist the perpetrators of a bust out scheme by revealing the credit limits and credit history for credit cards associated with the scheme. Defendant LODHI was listed as the "Manager" of Defendant LODHI's Business on the application for the Credit Report Company Account.

38. The Credit Report Company Account was used to check the credit reports for dozens of Fraudulent Cards. Many of these checks were done from Defendant LODHI's Residence, Defendant LODHI's Business, and Defendant BIBI's Residence. The vast majority of the individuals whose reports were accessed through the Credit Report Company Account were fictitious. Specifically, of the approximately 28 individuals whose reports were accessed through the Credit Report Company Account, all but three were fictitious.

**The Khan Account – An Example**

39. Between in or about September 2010 and in or about June 2011, a computer located at Defendant LODHI's Business was used to apply for numerous Fraudulent Cards.

40. Cookies have shown that a computer located at Defendant LODHI's Business created at least six different credit card applications for cards issued by just one Card Issuer – GE Money – alone. These approximately six applications were made in the names of six different individuals, using six different addresses. All of the applicants except one have been determined to be fictitious.[4]

41. One application, in the name of "Aazim Tawan," listed the address of Defendant LODHI's Business as Tawan's address. Based on a review of law enforcement and other databases, there is probable cause to believe that Aazim Tawan is a fictitious person. And, unsurprisingly, database checks have revealed that no one named Aazim Tawan has ever been employed by, or associated with, Defendant LODHI's Business.

42. Aside from these approximately six GE Money applications, another application, in the name of "Asad Khan," also used the address of Defendant LODHI's Business (the "Khan Application"). Based on a review of law enforcement and other databases, there is probable cause to believe that Asad Khan is a fictitious person.

43. The Khan Application was checked, through the Credit Report Company Account, exclusively from Defendant LODHI's Home and Defendant LODHI's Business.

**Bust Outs at Defendant LODHI's Business**

44. Defendant LODHI's Business has also been used to actually bust out several Fraudulent Cards.

45. For example, USAA issued a credit card ending in '3237 in the name of Ranjeet Dhillon (the "Dhillon Fraud Card"). Based on a review of law enforcement and other databases, there is probable cause to believe that Ranjeet Dhillon is a fictitious person.

46. The IP address that generated the Dhillon Fraud Card also generated approximately 10 other Fraudulent Cards issued by USAA alone.

47. The Dhillon Fraud Card was busted out at Defendant LODHI's Business. For example, on or about December 7, 2010, the Dhillon Fraud Card made a purchase of approximately $7,926.10 at a credit card merchant terminal located at Defendant LODHI's Business. Then, on or around December 10, 2010, the Dhillon Fraud Card mande another purchase, of approximately $7,457.94, at a merchant terminal located at Defendant LODHI's

[4] Records checks on the sixth applicant are incomplete.

Business. These charges have never been paid back, causing losses to USAA.

48. The total amount of bust outs made from the merchant terminal located at Defendant LODHI's Business is approximately $73,031, on approximately 5 different Fraudulent Cards.

**Proceeds from the Fraudulent Scheme**

49. As noted above, in or about April 2011, law enforcement officers seized approximately $2 million worth of jewelry from one of the Jersey City Jewelers, which had been obtained as part of the fraudulent scheme.

50. Moreover, defendants BIBI and LODHI have been seen in several luxury automobiles, including late-model Toyota Land Cruisers and Lexus brand sedans. Finally, the investigation has revealed that the defendants and others have purchased thousands of dollars of electronics, spa treatments, clothing, and accessories with proceeds from the Fraudulent Cards.