UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. MATTHEW MOSLEY	CASE NUMBER: **UNDER SEAL**

CRIMINAL COMPLAINT

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

From in or about October 2011 and continuing through in or about January 2012, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, United States Code, Section 1344	Defendant knowingly participated in a scheme to defraud financial institutions and to obtain money and funds owned by and under the custody and control of financial institutions by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of material facts, and for the purpose of executing such scheme, on or about October 18, 2011, caused the withdrawal of approximately $3,075 from an account belonging to Individual LR at Citibank, a financial institution whose deposits were insured by the Federal Deposit Insurance Corporation.

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

MARTIN J. NITSCHE
Postal Inspector
United States Postal Inspection Service

Sworn to before me and signed in my presence.

Date: October 24, 2014

Judge's signature

City and state: Chicago, Illinois

JEFFREY T. GILBERT, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS | ss

AFFIDAVIT

I, MARTIN J. NITSCHE, being duly sworn, state as follows:

1. I am a Postal Inspector with the United States Postal Inspection Service, and have been so employed since January 2008. My current responsibilities include the investigation of mail theft, access device fraud, bank fraud, and identity theft. Previously, I was a police officer in Orland Park, Illinois, for over ten years.

2. This affidavit is submitted in support of a criminal complaint alleging that, from in about October 2011 and continuing through in or about January 2012, MATTHEW MOSLEY participated in a scheme to defraud financial institutions, and to obtain money and property by means of materially false and fraudulent pretenses, representations, promises and by concealment of material facts, in violation of Title 18, United States Code, Section 1344 (bank fraud). Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging MOSLEY with bank fraud, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendant committed the offense alleged in the complaint.

3. This affidavit, and my knowledge of the bank fraud scheme described herein, is based on my personal knowledge; information provided to me by other law

enforcement agents; law enforcement interviews of individuals involved in the scheme, including individuals who provided their debit cards and Personal Identification Numbers for use in the scheme; information provided to law enforcement by bank investigators; information provided to law enforcement by victim businesses whose bank accounts have been compromised as a result of the scheme; covert operations by law enforcement to confirm the mechanics of the scheme and the identities of certain participants; and my review of records, including: (a) financial records and video surveillance provided by banks and credit unions, (b) currency exchange records, including video surveillance of debit card transactions, and (c) business records for debit and credit card processing companies.

FACTS SUPPORTING PROBABLE CAUSE

I. OVERVIEW OF THE CRACKING CARDS BANK FRAUD SCHEMES

4. The United States Postal Inspection Service and the Federal Bureau of Investigation, in conjunction with other local and federal law enforcement agencies and fraud investigators at several banks, have been investigating bank fraud schemes dubbed "Cracking Cards" by the participants. As detailed below, the investigation has determined that from approximately 2011 through the present, Cracking Cards schemers deposit counterfeit checks into bank accounts belonging to third parties who willingly or unwillingly surrender their debit cards and PINs for use in the schemes. The schemers then use Automated Teller Machines or point of sale terminals at currency exchanges and retail stores to withdraw or spend funds

that the banks advance to the third-party accounts before learning the counterfeit nature of the deposited checks. The banks suffer losses when the checks are found to be counterfeit, and the third-party account holders deny responsibility for the withdrawals and purchases.

5. Based on the investigation by Postal Inspectors, the FBI, and other law enforcement agencies, and my training and experience, I understand that the Cracking Cards bank fraud schemes generally work as follows:

A. Schemers Recruit Bank Account Holders to Provide Their Debit Cards and PINs

6. Law enforcement has obtained information about the operation of the Cracking Cards schemes from, among other sources, a Cooperating Witness. The CW has been charged by complaint in the Northern District of Illinois in relation to the CW's involvement in a Cracking Cards scheme. The government's preliminary calculation of actual losses attributable to the CW in conjunction with Cracking Cards is over $400,000. The CW is cooperating with law enforcement with the hope that his cooperation will be considered by the government in recommending a lower sentence. The CW has no prior criminal convictions. In addition, information provided by CW has been corroborated through witness interviews and review of financial records. I believe that the CW has provided reliable information about Cracking Card schemes.

7. According to the CW and numerous individuals who have provided their debit cards and PINs for use in the scheme, Cracking Cards schemers recruit

bank account holders to give up their debit cards and PINs by promising the account holders a portion of the profits.

8. According to the CW and to individuals who were recruited to give up their debit cards, the methods of recruitment vary depending on the schemer. Some recruit card holders in person, such as at a party, at school, or on the street. Others use social media outlets such as Instagram and Facebook to advertise opportunities for making fast cash, after which account holders contact the Cracking Cards schemer by phone and listen to the schemer's pitch. Some schemers work together in pairs or groups in their recruitment efforts.

B. Schemers Purchase or Manufacture Counterfeit Checks

9. According to the CW, once a Cracking Cards schemer has a debit card and PIN for a third-party account, the schemer manufactures, purchases, or otherwise obtains one or more counterfeit checks to deposit into the third-party bank account. As explained by the CW and corroborated by bank records and interviews of victim businesses, the counterfeit checks used in Cracking Cards schemes generally contain legitimate bank account and routing numbers that belong to the accounts of actual business entities.[1]

10. According to the CW, the combination of a legitimate bank account number and routing number, as well as the name and address of the victim

[1] On occasion, a schemer will use a fictitious account number on a counterfeit check. Banks often float or advance the funds on a check deposit before the account number is verified and the check is cleared.

business, is referred to by those involved in Cracking Cards as the bank account "profile" for that business.

11. According to the CW, and as confirmed through undercover purchases of counterfeit checks from Cracking Cards schemers, not everyone who "cracks cards" manufactures his or her own counterfeit checks to deposit into third-party accounts. Rather, certain individuals have a reputation for "making paper," that is, making and printing counterfeit checks. The people who "make paper" sell counterfeit checks to others involved in Cracking Cards. The CW explained that he "made paper" for his own use and for selling to others who cracked cards, by using a computer software program. Participants who "make paper" obtain business profiles (bank account and routing numbers) through a variety of unauthorized and illegal means.

C. Schemers Deposit Counterfeit Checks into Third-Party Bank Accounts

12. According to the CW, once a Cracking Cards schemer has secured a third-party debit card and PIN, as well as one or more counterfeit checks, the schemer deposits—or recruits someone else to deposit—the counterfeit checks into the third party's bank account, typically via an ATM transaction. As corroborated by bank records, the Cracking Card schemer then waits for the account holder's bank to credit the purported funds from the counterfeit check, which can happen within a matter of hours.

13. According to information provided by bank investigators, banks credit the value of a check to a card holder's account before the check clears, that is, before

the cardholder's bank receives an image of the check (which is sent electronically to the drawer's bank), determines whether it is valid, and requests and receives payment (or denial of payment) from the check drawer's bank. In effect, the cardholder's bank advances the bank's own money into the cardholder's account when a check is deposited—even if it is a counterfeit or fraudulent check. During the time period between the deposit of a fraudulent check and when the cardholder's bank learns that the check is fraudulent, the advanced money in the cardholder's bank account can be withdrawn using the cardholder's debit card.

D. Schemers Withdraw or Spend Funds from the Third-Party Bank Account

14. According to the CW and as corroborated by bank records, after one or more counterfeit checks are deposited into a third-party bank account, the Cracking Cards schemer often attempts a relatively small ATM withdrawal (between $100 and $500) a few hours later, to determine whether the bank has credited the account with the purported funds from the counterfeit check. If the schemer is able to withdraw the cash at an ATM, (i.e., the bank has advanced funds to the account), the schemer goes to a point-of-sale terminal to withdraw or spend the remaining funds that the bank advanced to the third-party account because of the deposit of the counterfeit checks. Point-of-sale terminals are machines used to process debit and credit card payments, typically for the purchase of goods. For example, the machines at a grocery store checkout counter in which a customer swipes a debit card are point of sale terminals.

E. Loss to Financial Institutions

15. When floated funds are withdrawn in person at a bank branch, or at a bank ATM, as a result of a counterfeit check deposit, the bank suffers the loss when it hands the cash over to the person or disperses it out of the machine. When floated funds are withdrawn or spent at a point-of-sale terminal, casino, or retail store, the bank suffers the loss through a series of electronic funds transfers that are managed by a debit card processing service, similar to the Automated Clearing House, but for debit transactions as opposed to credit transactions. The purchase is premised on the customer entering the correct PIN into the keypad at the store/currency exchange (the point-of-sale terminal). A communication goes from the point-of-sale terminal to the terminal's processing company, which electronically communicates with the customer's bank via the debit-processing network to verify that the PIN is accurate and that the account and its funds are accessible. At that point in the process, it is the customer's bank, via the debit-processing network, that makes the decision whether the purchase can go through. If the bank approves the purchase, the bank is agreeing to pay back the store/currency exchange the amount of the purchase. If the purchase is approved, the store/currency exchange then hands over the product to the customer (e.g., a television, or in the case of the currency exchange, cash).

16. According to the CW, Cracking Cards schemes are popular methods to obtain illicit funds and defraud banks in City of Chicago, and are carried out by numerous schemers, including those affiliated with Chicago gangs.

II. FACTS CONCERNING CURRENCY EXCHANGE A

17. Between November 2011 and September 2014, Postal Inspectors and the FBI, among other law enforcement agencies, have monitored and investigated Cracking Cards transactions at Currency Exchange A, located in Chicago, Illinois. Through this investigation, law enforcement agents have obtained information about suspicious transactions linked to a Cracking Cards scheme, and in particular, withdrawal transactions from Currency Exchange A's point of sale terminals that followed the deposit of counterfeit checks into the respective card holder bank accounts.

18. According to Currency Exchange A's Chief Operating Officer, starting in or around January 2012, for debit transactions of $1,000 or more, the Currency Exchange A's processing software required that a customer profile be electronically attached to the transaction.[2] A customer profile was stored electronically on the computer system and contained the customer's personal identify information which included his/her name, social security number, date of birth, address, and phone number. Almost all profiles included a scanned image of a driver's license or state identification card and some also contained a web camera photo of the customer. Thus, if a customer wanted to use a point of sale terminal to withdraw funds from a

[2] According to Currency Exchange A's computer records, there is only one withdrawal transaction for over $1,000, on January 5, 2012, that was processed under MOSLEY's electronic profile. As outlined below in paragraph 35, MOSLEY's other withdrawals at Currency Exchange A happened before Currency Exchange A's computer system required that withdrawals exceeding $1,000 be processed under the customer's electronic profile.

debit card for $1,000 or more, the teller[3] had to enter the individual's personal identifying information into the computer system before the teller could proceed with the debit card transaction. Once the teller entered identifying information, such as a name or date of birth, the computer system pulled up the customer's electronic profile, which contained a photograph of the person. Before proceeding with a debit card withdrawal over $1,000, the teller was required to compare the profile picture on the screen with the customer standing at the teller window. Only after confirming the customer's identity on the teller's computer could the teller could proceed to the next screen and move forward with the debit card withdrawal.[4]

19. According to Currency Exchange A's Chief Operating Officer, if the customer had no profile in the currency exchange's computer system, the teller had to set up a customer profile before proceeding, which required scanning the

[3] Approximately five tellers from Currency Exchange A have informed law enforcement that they regularly accepted tips ranging from approximately $10-200 from customers who made withdrawals from debit cards (as well as from customers who conducted other business at Currency Exchange A). Currency Exchange A's Chief Operating Officer informed law enforcement that the tellers were permitted to accept voluntary tips from customers.

[4] Based on law enforcement's review of over 350 videos of withdrawal transactions at Currency Exchange A and the corresponding records, there are approximately 11 known instances in which it appears that one teller (Teller A) processed a debit card withdrawal under the electronic customer profile for an individual other than the person who was standing at the teller window making the withdrawal. Law enforcement has no information that any teller other than Teller A processed any debit card withdrawal under an incorrect electronic customer profile. Also, at least one witness provided information that Teller A accepted tips of up to $200, whereas Teller A reported to law enforcement that the maximum tip she received was approximately $100. However, even if any of the three withdrawal transactions outlined in paragraphs 24-35, below, involved Teller A, video surveillance evidence for these three transactions confirms that MOSLEY was the person making those withdrawals, consistent with the electronic customer profile for MOSLEY.

customer's State-issued photo-ID and entering the customer's personal identifying information into the computer system.

20. In addition, according to Currency Exchange A's Chief Operating Officer, beginning on November 15, 2011, the tellers were required to maintain a handwritten log of debit withdrawals over $1,000 by recording the customer's name, the last four digits of the debit card number, and the amount of the withdrawal.[5]

21. During the investigation, law enforcement agents have obtained: (1) video surveillance of these transactions at Currency Exchange A, (2) the handwritten log of point-of-sale transactions maintained by tellers for transactions over $1,000, (3) Currency Exchange A's profile of its customers, which includes the customers' name and copies of their driver's license; and (4) Currency Exchange A's transaction records for point-of-sale cash withdrawals.

III. FACTS CONCERNING MATTHEW MOSLEY

22. The investigation has determined that there is probable cause to believe that MATTHEW MOSLEY has participated in the Cracking Cards scheme. In total, from in or about October 2011 through in or about January 2012, law enforcement agents have reviewed bank records for five bank accounts belonging to individuals other than MOSLEY, from which MOSLEY withdrew funds following one or more deposits of counterfeit checks. In total, the banks affected by withdrawals of funds from these five accounts suffered losses in excess of $32,000.

[5] According to Currency Exchange A's handwritten log, there was only one withdrawal transaction for over $1,000, on January 5, 2012, that was attributed to MOSLEY. As outlined below in paragraph 35, MOSLEY's other withdrawals at Currency Exchange A happened before Currency Exchange A implemented the handwritten log.

23. According to the CW, MOSLEY "makes paper" for Cracking Cards. That is, MOSLEY manufactures counterfeit checks for use in Cracking Cards schemes. The CW reported that he purchased counterfeit checks from MOSLEY. Also according to the CW, MOSLEY sells counterfeit checks to other individuals who then use those counterfeit checks in Cracking Card schemes.

A. Withdrawal Transaction from Individual TM's Bank Account on or about November 2, 2012

24. According to Citibank account records for an account belonging to Individual TM, on November 1, 2011, at approximately 11:20 a.m., a check in the amount of $3,524.68 (check number 217652), drawn on an account purportedly belonging to Company DI and purportedly drawn on a bank account for the "State Treasurer of Illinois," made payable to Individual TM, was deposited into a savings account ending in 3488 belonging to Individual TM. Prior to this deposit, the balance in Individual TM's account ending in 3488 was -$12.26. Also according to Citibank account records, on November 1, 2011, a check in the amount of $3,584.09 (check number 217653), drawn on an account purportedly belonging to Company DI and purportedly drawn on an account for the "State Treasurer of Illinois," made payable to Individual TM, was deposited into a checking account ending in 2992 belonging to Individual TM. Prior to this deposit, the balance in Individual TM's account ending in 2992 was $0.00. Citibank records show that these checks were rejected on November 4, 2011. Citibank records also show that a debit card ending in 5121 was the debit card for Individual TM's accounts ending in 3488 and 2992.

25. According to information provided by a representative for Company DI, the checks that were deposited into Individual TM's accounts on November 1, 2011, (check numbers 217652 and 217653) were counterfeit checks not issued by or authorized by Company DI.

26. I have reviewed a photograph excerpted from Citibank's video surveillance of the November 1, 2011, deposits of Company DI checks into Individual TM's accounts, and compared it to an Illinois driver's license photograph of MOSLEY. I recognize MOSLEY as the individual who made these deposits.

27. Citibank records also show that, on November 2, 2011, at 6:14 a.m., there was an ATM transfer of $3,400 from Individual TM's account ending in 3488, into Individual TM's account ending in 2992. I have reviewed photographs excerpted from Citibank's video surveillance of this ATM transfer and compared them to an Illinois driver's license photograph of MOSLEY. I recognize MOSLEY as the individual who conducted this ATM transfer.

28. According to Citibank records for Individual TM's account ending in 2992, on November 2, 2011, at 6:51 a.m., there was a withdrawal of $2,770.42 at Currency Exchange A, using Individual TM's debit card ending in 5121.

29. I have reviewed Currency Exchange A's debit card processor's records for November 2, 2011, which show a withdrawal of $2,770.42 at Currency Exchange A, at 6:51 a.m., using the debit card ending in 5121 that matches the debit card for Individual TM's accounts.

30. I have reviewed a copy of the surveillance video from Currency Exchange A from November 2, 2011. From my review of the surveillance video and my comparison to an Illinois driver's license photograph of MOSLEY, I recognize MOSLEY as the individual who made the withdrawal of $2770.42 from Individual TM's account ending in 2992. The time stamp on the video surveillance from Currency Exchange A is approximately 6:51 a.m.

31. Using debit card processor records and bank statements obtained during the investigation, I have determined that MOSLEY made the withdrawal on November 2, 2011, from an account belonging to Individual TM, and not an account belonging to MOSLEY.

32. Citibank records for Individual TM's account further reflect that this withdrawal occurred after the deposit of the Company DI checks purportedly drawn on a "State Treasurer of Illinois" bank account, on November 1, 2011, but before those check deposits were rejected.

33. According to a representative from Citibank, the bank advances its own funds into customers' bank accounts the next business day after the deposit of checks so that customers can withdraw funds without waiting for checks to clear.

B. Additional Cracking Cards Transactions for MOSLEY

34. I have also reviewed transactions relating to four additional bank accounts belonging to individuals other than MOSLEY. For each of these accounts, I have reviewed bank records that show one or more deposits of counterfeit checks into the respective individuals' bank accounts, followed by withdrawals at ATMs or

Currency Exchange A. Additionally, I have reviewed surveillance video or photographs relating to each account, showing either the deposit of a counterfeit check, or the withdrawal of funds following the deposit of a counterfeit check. Based on my comparison to an Illinois driver's license photograph of MOSLEY, I recognize MOSLEY as the individual who either deposited a counterfeit check into these accounts, or withdrew funds from these accounts following such a deposit.

35. Additionally, for these transactions I have confirmed the following information: (1) the checks were deposited into accounts that did not belong to MOSLEY; (2) the deposited checks were all rejected by the drawer bank within days after the deposits; (3) the deposited checks constituted most, if not all, of the funds in the accounts; (4) withdrawals from these accounts were funded by the deposited counterfeit checks; (5) the banks that authorized the withdrawals advanced funds into the individuals' accounts before the deposited checks cleared.

Account Holder	Deposit Date	Check(s) Deposited	Surveillance of Mosley	Withdrawal Date	Withdrawal Location	Withdrawal Amount	Surveillance of Mosley
LR	10/17/2011	$3,842.69	Yes	10/18/2011	Currency Exchange A	$3,075	Yes
TJ	11/2/2011	$2,976.36 $3,069.82	Yes	11/3/2011	Citibank ATM	$500.00 $500.00	Yes
KC	11/2/2011	$3,719.21		11/3/2011	Citibank ATM	$520.00 $100.00	Yes
UB	1/4/2012	$3,692.32		1/5/2012	Currency Exchange A	$3,750.00	Yes

IV. FDIC INFORMATION

36. I have obtained a certificate issued by the Federal Deposit Insurance Corporation that confirms that the deposits of Citibank were insured by the Federal Deposit Insurance Corporation between October 2011 and January 2012.

V. CONCLUSION

36. Based upon the information set forth in this affidavit, I believe there is probable cause to believe that, from in or about October 2011 and continuing through in or about January 2012, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, MOSLEY knowingly participated in a scheme to defraud a financial institution and to obtain money and funds owned by and under the custody and control of a financial institution by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of material facts, and, for the purpose of executing such scheme, on or about November 2, 2011, caused the withdrawal of approximately $2,770.42 from an account belonging to Individual TM at Citibank, a financial institution whose deposits were insured by the FDIC, in violation of Title 18, United States Code, Section 1344 (bank fraud).

FURTHER AFFIANT SAYETH NOT.

MARTIN J. NITSCHE
Postal Inspector
United States Postal Inspection Service

SUBSCRIBED AND SWORN to before me on October 24, 2014.

JEFFREY T. GILBERT
United States Magistrate Judge