

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

MEDFORD DIVISION

FILED 16 FEB 4 13 37 USDC-OR

1:16-CR-00062-AA

UNITED STATES OF AMERICA,

INDICTMENT (UNDER SEAL)

v.

Count 1: 18 U.S.C. § 1349
Conspiracy to Commit Mail Fraud

MICHAEL OLUWASEGUN KAZEEM,

Counts 2 through 8: 18 U.S.C. § 1341
Mail Fraud

Defendant,

Counts 9 through 15: 18 U.S.C. § 1028A
Aggravated Identity Theft

Forfeiture Allegations:
18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. §
2461(c)

THE GRAND JURY CHARGES:

COUNT 1

(CONSPIRACY TO COMMIT MAIL FRAUD)

INTRODUCTION

At all times material to this Indictment:

1. As set forth below, defendant's and his co-conspirator's conduct involved obtaining stolen personal identifying information of more than 250,000 individuals and, beginning as early as the 2012 tax year to May 2015, using that information to file fraudulent federal tax returns. In total, defendant and his co-conspirators filed over 2,900 false federal tax returns seeking over

\$25 million dollars in fraudulent refunds. The actual loss exceeded \$4.7 million dollars from tax returns accepted for payment by the Internal Revenue Service (IRS).

2. Defendant **MICHAEL OLUWASEGUN KAZEEM**, also known by online monikers “micjoh94@xxx.com” aka “Mic Joh” and “ed.thm87@xxx.com” aka Edith Thomas, resides in Nigeria and the state of Georgia.

3. Defendant’s brother, Emmanuel Oluwatosin Kazeem (E. Kazeem), also known by online monikers “philipe1212@xxx.com,” aka “Paka Phil,” “Philippe Philipe” and “Paka Philipe” and “princephilipe1212@xxx.com” aka “Prince Phil,” resides in Maryland.

4. Oluwamuyiwa Abolad Olawoye (Olawoye), also known by online moniker “macktomson20@xxx.com,” aka “land smith” resides in Georgia.

5. The term “Personal Identifying Information” or “PII,” can include an individual’s name, address, social security number, date of birth, places of work, duration of work, state driver’s license number, mother’s maiden name, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.

6. For tax purposes, an “Electronic Filing PIN” is a five digit personal identification number that is required for electronically filing tax returns with the IRS when the filer does not have a Self-Select PIN or know his or her Adjusted Gross Income from the previous year. Using the website IRS.gov, a filer can request an Electronic Filing PIN by authenticating his or her purported identity by entering a host of personal information, including social security number, full name, date of birth, filing status, and full address.

7. A “means of identification” is any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including a name, Social Security number, date of birth, or an access device. 18 U.S.C. § 1028(d)(7).

8. An “access device” is, among other things, any card, account number, or other means of account access, that could be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that could be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument), including a prepaid debit card or prepaid debit card account number. 18 U.S.C. § 1029(e)(1).

9. A “prepaid debit card” is a card linked to an account at a financial institution, which could be used to receive deposits electronically, like a traditional bank account, and to make purchases and cash withdrawals with funds in the account, like a traditional debit card. Prepaid debit cards are administered through many providers, including but not limited to Green Dot Bank.

10. A “disposable email address” is an email address that is given to specified senders and typically used to forward incoming emails to one or more permanent email addresses where the owner receives and reads messages. It may be used as a means of shielding a permanent email address from senders and it can protect the integrity of a permanent email address because the disposable address may be canceled at any time without the owner changing his or her permanent email address. A disposable email address also includes an email address obtained from a service provider without revealing the users true identity and is used for a particular, limited purpose, thereafter to be discarded or not otherwise used for other purposes.

11. The term “IRS transcript” is taxpayer information that shows the taxpayer’s tax return information filed with the IRS including line items from the return filed and basic data, such as marital status, type of return, adjusted gross income and taxable income. It also shows information reported to the IRS such as on W-2, 1099 and 1098 forms. IRS transcripts were available online through the IRS “Get Transcript” application, a multi-step authentication

process using the taxpayer's personal identifying information that is provided such as Social Security number, date of birth, tax filing status and home address as well as answers to personal identity verification questions designed to elicit information that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

THE CONSPIRACY

12. Beginning as early as tax year 2012, the exact date being unknown to the Grand Jury, and continuing to May 2015, in the District of Oregon and elsewhere, defendant **MICHAEL OLUWASEGUN KAZEEM**, unlawfully and knowingly conspired and agreed with E. Kazeem, Olawoye and with other persons both known and unknown to the Grand Jury, to commit Mail Fraud by knowingly and willfully using or causing the use of the United States mails or private or commercial interstate carrier in furtherance and execution of a material scheme or artifice to defraud and obtain money by means of materially false and fraudulent pretenses and representations in violation of Title 18, United States Code, Sections 1341 and 1349.

Objects of the Conspiracy/Scheme to Defraud

13. It was the object of the conspiracy and the scheme to defraud to obtain stolen PII and use that identifying information, as well as false information relating to employment and income, for the purpose of preparing and electronically filing fraudulent tax returns with the Internal Revenue Service claiming fraudulent refunds. It was also an object of the conspiracy to obtain the fraudulent refunds associated with those fraudulent returns through direct deposits to debit cards fraudulently registered with the stolen PII.

/

/

Stolen Identity Information

14. It was part of the conspiracy that the defendant and his co-conspirators obtained the names and other personal identifying information that belonged to United States taxpayers, without their knowledge or consent, by unauthorized means including the purchase of the stolen information. The stolen PII belonged to over 250,000 people and included stolen PII originating from a database owned by a pre-employment and volunteer background check company located in Oregon (the "Oregon Database").

15. It was a further part of the conspiracy that the defendant and his co-conspirators, using email and instant messenger accounts, exchanged hundreds of communications containing the stolen social security numbers and other PII of over 83,000 individuals whose information originated from the Oregon Database. This included over 40,500 residents from Oregon. Some of the specific emails exchanged as part of the conspiracy included the following:

- a. On or about February 1, 2014, defendant and E. Kazeem exchanged emails containing stolen PII for Oregon resident J.M. and Washington resident M.M.
- b. On or about February 9, 2014, defendant and E. Kazeem exchanged emails containing stolen PII for Oregon resident A.T.
- c. On or about February 20, 2014, defendant and E. Kazeem exchanged emails containing stolen PII for Oregon residents A.B. and B.L.

16. It was a further part of the conspiracy that the following number of stolen identities for use in carrying out their fraudulent scheme were obtained by defendant and two of his co-conspirators:

- a. **Defendant:** over 16,500 (with over 10,500 from the Oregon Database and over 5,000 of those belonging to residents of Oregon);

- b. E. Kazeem: over 120,000 (with over 81,000 from the Oregon Database and over 39,500 of those belonging to residents of Oregon); and,
- c. Olawoye: over 111,500 (with over 11,500 from the Oregon Database and over 5,000 of those belonging to residents of Oregon).

IRS Transcripts

17. It was part of the conspiracy that the defendant and his co-conspirators used the stolen PII for unauthorized access into the Internal Revenue Service system to obtain over 1,200 taxpayer transcripts from the IRS.

18. It was a further part of the conspiracy that the IRS transcripts were obtained for the named taxpayers whose PII was stolen for subsequent use in filing fraudulent tax returns in their names.

19. It was a further part of the conspiracy that defendant and his co-conspirators, using email and instant messenger accounts, had communications containing both disposable email addresses that were used in obtaining IRS transcripts and stolen IRS transcript information of individual taxpayers whose information was used in obtaining fraudulent tax returns. Some of the specific emails exchanged as part of the conspiracy included the following:

- a. On or about February 8, 2015, defendant transmitted to E. Kazeem disposable email addresses that were later used for obtaining over 725 IRS transcripts of individual taxpayers.
- b. On or about April 7, 2015 Olawoye transmitted stolen IRS transcript information to defendant.

Electronic Filing PINs

20. It was part of the conspiracy that the defendant and his co-conspirators used the stolen PII to obtain Electronic Filing PINs from the Internal Revenue Service.

21. It was a further part of the conspiracy that the Electronic Filing PINs were acquired in the names of individuals whose PII was stolen for subsequent use in filing fraudulent tax returns in their names.

22. It was a further part of the conspiracy that defendant and his co-conspirators, using email and instant messenger accounts, had communications containing the Electronic Filing PINs and stolen taxpayer PII for use in obtaining fraudulent tax returns. This included defendant sending E. Kazeem over 4,000 fraudulently obtained Electronic Filing PINs. Some of the specific emails exchanged as part of the conspiracy included the following:

- a. On or about February 9, 2014, defendant sent E. Kazeem an email containing Electronic Filing PINs fraudulently obtained from the IRS for Oregon residents J.M. and A.T., and Washington residents C.G., M.C. and C.S.
- b. On or about February 10, 2014, defendant sent E. Kazeem an email containing Electronic Filing PIN fraudulently obtained from the IRS for Oregon resident C.D.
- c. On or about February 20, 2014, defendant sent E. Kazeem an email containing Electronic Filing PIN fraudulently obtained from the IRS for Oregon resident A.B.

23. As part of the conspiracy, for tax year 2013, the fraudulent Electronic Filing PINs defendant sent to E. Kazeem were used to file over 900 fraudulent federal tax returns claiming refunds in excess of \$8.5 million dollars. The actual loss exceeded \$2.4 million dollars from the fraudulent tax returns accepted for payment by the IRS.

Prepaid Debit Cards

24. It was part of the conspiracy that the co-conspirators obtained debit and/or other stored value cards for the purpose of receiving direct deposits of fraudulent tax refunds including, but not limited to, Green Dot debit cards issued by Green Dot Bank, a financial institution.

25. It was a further part of the conspiracy that the co-conspirators purchased Green Dot temporary prepaid debit cards at various retail locations. In order to receive direct deposit funds, including the direct deposit of federal tax refunds, the co-conspirators “personalized” the cards by registering them with Green Dot, as required. As part of the registration process, they provided Green Dot with stolen PII including the names and mailing addresses of those individuals resulting in Green Dot mailing personalized-registered cards via U.S. mail to the mailing addresses and in the registered names provided by the co-conspirators. Upon registration, and in order to receive direct deposits of tax refunds, the co-conspirators also obtained the Green Dot Bank routing number and the Direct Deposit Account number created from the Primary Card Reference number linked to the number embossed on both the original-temporary card and the personalized-registered card.

Disposable Email Addresses

26. It was part of the conspiracy that the co-conspirators used disposable email addresses for use in filing fraudulent tax returns, registering prepaid debit cards in the names of the individuals whose PII was stolen, and to further conceal their fraudulent scheme. As part of the conspiracy, for tax year 2013, the disposable email addresses defendant provided to E. Kazeem were used to file over 460 fraudulent federal tax returns claiming fraudulent refunds in excess of \$2.5 million dollars. The actual loss exceeded \$100,000 from tax returns accepted for payment by the IRS.

Obtaining Fraudulent Refunds

27. It was part of the conspiracy that the co-conspirators electronically filed false and fraudulent individual tax returns with the IRS claiming that fraudulent tax refunds were owed.

28. It was a further part of the conspiracy that the co-conspirators used the stolen names and other PII, and any IRS transcript information that was acquired, to create the fraudulent income tax returns and false Form W-2 Wage and Tax statements, which contained fictitious information regarding employment, wages, withholding, and tax credits. Whenever the co-conspirators filed a fraudulent tax return that was rejected by the IRS for payment, the co-conspirators often created another fraudulent tax return after changing some of the information from the initial rejected return and refiling the newly created return in an effort to have it accepted for payment.

29. It was a further part of the conspiracy that defendant and his co-conspirators used the fraudulent Electronic Filing PINs defendant sent to E. Kazeem as well as some of the disposable email addresses to file fraudulent federal tax returns. As part of the conspiracy, it included filing approximately 1,375 fraudulent federal tax returns for tax year 2013 with those Electronic Filing PINs and disposable email addresses claiming fraudulent refunds in excess of \$11 million dollars. The actual loss exceeded \$2.6 million dollars from tax returns accepted for payment by the IRS.

30. It was a further part of the conspiracy that the co-conspirators acquired and used hundreds of Green Dot debit cards using the stolen PII to receive fraudulent tax refunds. The co-conspirators included the Direct Deposit Account number along with a Green Dot Bank routing number provided to them at the time of registration on the fraudulently filed tax return to initiate the direct deposit of the fraudulent refunds to the Green Dot Account. The co-conspirators subsequently accessed those funds from the original-temporary card.

31. It was a further part of the conspiracy that the co-conspirators exchanged information regarding the Green Dot account numbers and the anticipated fraudulent tax refunds associated with those accounts. It also involved the recruitment of other co-conspirators to acquire Green Dot cards and assist in the obtaining and disposing of the fraudulent IRS tax return funds including, but not limited to, an exchange of emails between defendant and E. Kazeem, on or about September 1, 2013, in which they discussed arranging for the use of a person recruited from Las Vegas, Nevada in the scheme who would be paid \$500 for each card that had fraudulent tax refunds successfully placed on it with the remaining fraudulent proceeds being wired to Nigeria by means of Western Union.

32. It was a further part of the conspiracy that the co-conspirators passed information in coordination with the acquisition of Green Dot debit cards, the filing of fraudulent tax returns and the obtaining of fraudulent refunds including, but not limited to, the following:

- a. On February 18, 2014, E. Kazeem emailed the stolen PII of Oregon residents A.B. and B.L. contained in the Oregon Database to the defendant. On February 20, 2014, defendant emailed the stolen PII of A.B. and B.L. along with a fraudulently acquired IRS Electronic Filing PIN for each one to E. Kazeem.
- b. On or about February 21, 2014, the co-conspirators purchased a temporary Green Dot card and registered it in the name of A.B. whereupon Green Dot mailed the personalized Green Dot card to A.B. at the Corvallis, Oregon address associated with A.B. pursuant to the co-conspirator's direction.
- c. On February 21, 2014, the co-conspirators filed a fraudulent federal tax return in the names of A.B. and B.L. The fraudulent return contained accurate stolen PII for both A.B. and B.L. and claimed a \$9,687 refund to be directly deposited into the

account associated with the Green Dot card registered in the name of A.B. After the IRS paid the refund, the co-conspirators withdrew the funds using the original-temporary Green Dot card still in their possession.

33. It was a further part of the conspiracy that the co-conspirators retrieved the acquired fraudulent tax refunds from the debit and/or stored value cards through various purchases, including the purchase of money orders or wire transfers payable to the co-conspirators and converted cash and money orders for the personal use of the co-conspirators.

34. Defendant and his co-conspirators took steps to conceal the existence of the conspiracy.

Additional Overt Acts in Furtherance of the Conspiracy

35. In furtherance of the conspiracy, and to effect, promote and accomplish the objects of it, defendant and other persons known and unknown to the Grand Jury, caused to be committed, among others, the use of the United States mail, or private or commercial interstate carrier, set forth in Counts 2 through 8 of this Indictment, incorporated herein by this reference.

All in violation of Title 18, United States Code, Section 1349.

COUNTS 2-8

(MAIL FRAUD)

36. Paragraphs 1 through 34 of the Indictment are re-alleged and incorporated herein by reference.

37. On or about the dates listed below, in the District of Oregon and elsewhere, defendant **MICHAEL OLUWASEGUN KAZEEM**, together with persons known and unknown to the Grand Jury, having knowingly and intentionally devised a material scheme and artifice to defraud the Internal Revenue Service and obtain money from the United States Treasury by means of materially false and fraudulent pretenses and representations, and for the purpose of

executing the aforementioned material scheme and artifice, and attempting to do so, did knowingly cause debit cards, as described below, to be placed in a post office and authorized depository for mail matter, and delivered by the United States Postal Service (USPS) or private or commercial interstate carrier to the mailing addresses described below, each use of the mails being a separate count of this Indictment:

Count	Date of Offense	Mailing
2	On or about 02/13/2014	Debit card in the name of J.M., addressed to J.M. in Portland, Oregon.
3	On or about 02/13/2014	Debit card in the name of A.T., addressed to A.T. in Portland, Oregon.
4	On or about 02/13/2014	Debit card in the name of C.G., addressed to C.G. in Portland, Oregon.
5	On or about 02/13/2014	Debit card in the name of M.C., addressed to M.C. in Portland, Oregon.
6	On or about 02/13/2014	Debit card in the name of C.D., addressed to C.D. in Portland, Oregon.
7	On or about 02/21/2014	Debit card in the name of A.B., addressed to A.B. in Corvallis, Oregon.
8	On or about 04/25/2014	Debit card in the name of C.S., addressed to C.S. in Salem, Oregon

All in violation of Title 18, United States Code, Section 1341.

/

/

/

COUNTS 9-15

(AGGRAVATED IDENTITY THEFT)

38. On or about the dates listed below, in the District of Oregon and elsewhere, defendant **MICHAEL OLUWASEGUN KAZEEM**, together with persons known and unknown to the Grand Jury, did knowingly possess, transfer and use, without lawful authority, the means of identification of another person including the name, Social Security number, and other stolen personal identifying information of an actual person known to the Grand Jury, listed by his or her initials below, during the registration process of prepaid debit cards that occurred during and in relation to the commission of a federal felony enumerated in 18 U.S.C. § 1028A(c), to wit: mail fraud and conspiracy to commit mail fraud in violation of Title 18, United States Code, Sections 1341 and 1349 as alleged in the related fraud Counts of this Indictment referenced below, each use of the mails being a separate count of this Indictment:

Count	Date of Offense	Related Fraud Counts	Individual
9	On or about 02/13/2014	1 and 2	J.M.
10	On or about 02/13/2014	1 and 3	A.T.
11	On or about 02/13/2014	1 and 4	C.G.
12	On or about 02/13/2014	1 and 5	M.C.
13	On or about 02/13/2014	1 and 6	C.D.
14	On or about 02/21/2014	1 and 7	A.B.
15	On or about 04/25/2014	1 and 8	C.S.

All in violation of Title 18, United States Code, Sections 1028A(a)(1), (c)(5).


FORFEITURE ALLEGATION

39. Upon conviction of one or more of the offenses set forth in Counts 1 through 8 of this Indictment, defendant **MICHAEL OLUWASEGUN KAZEEM** shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28 United States Code, Section 2461(c), any and all property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violations.

Dated this 4th day of February 2016.

A TRUE BILL.

Presented by:
BILLY J. WILLIAMS
United States Attorney


BYRON CHATFIELD
Assistant United States Attorney