

UNITED STATES DISTRICT COURT

LOGGED RECEIVED

for the

JAN - 2 2019

District of Maryland

AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND

United States of America)

v.)

KENO ROMARIO BROWN)

Case No. GLS-19-00001

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of April 2013 through March 2018 in the county of Prince George's & elsewhere in the District of Maryland, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 1349; 1029(b)2); 1028A	Wire fraud; Conspiracy to commit wire fraud; Aggravated Identity Theft

This criminal complaint is based on these facts:

See attached affidavit.

Continued on the attached sheet.

Courtney L. Mulholland
Complainant's signature

Courtney L. Mulholland, United States Postal Inspector
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/2/19

Gina L. Simms
Judge's signature

City and state: Greenbelt, Maryland

Hon. Gina L. Simms, U.S. Magistrate Judge
Printed name and title

FILED ENTERED
LODGED RECEIVED

GDB/DJB: USAO 2012R00709

JAN - 2 2019

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

AT GREENBELT
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND



UNITED STATES OF AMERICA

v.

KENO ROMARIO BROWN,

Defendant

*
*
*
*
*
*
*
*
*
*

CASE NO. *GLS-19-00001*

(Wire Fraud Conspiracy,
18 U.S.C. § 1349; Conspiracy to
Commit Access Device Fraud,
18 U.S.C. § 1029(b)(2); Aggravated
Identity Theft, 18 U.S.C. § 1028A)

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Courtney Mulholland, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of a criminal complaint and an arrest warrant. Based on the following facts, there is probable cause to believe that **KENO ROMARIO BROWN** ("**BROWN**") has violated federal criminal statutes, including conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2); and aggravated identity theft, in violation of 18 U.S.C. § 1028A.

2. I have been a United States Postal Inspector since May 2003. I am currently assigned to the Washington, D.C. division of the Mail Fraud Team, Washington Division. In that capacity, I investigate allegations of criminal fraud involving the use of the United States mail. I have experience investigating fraud and identity theft. I derived the facts in this affidavit from my personal observations, my training and experience, and information obtained from other agents and witnesses. I intend this affidavit only to show that there is sufficient probable cause for the requested warrant.

PROBABLE CAUSE

Introduction

3. The Federal Bureau of Investigation (“FBI”) and the United States Postal Inspection Service (“USPIS”) (“the government”) are conducting an investigation into individuals perpetrating an “advance fee scheme,” where the coconspirators contact victims—who are almost always senior citizens—and falsely represent to the victims that they won a lottery or sweepstakes and need to send money for taxes and fees in order to receive the prize. The prizes are not real and the coconspirators have never been employees of a legitimate lottery or sweepstakes.

4. To execute the scheme, the coconspirators persuade their victims to pay the advance fees and taxes by sending cash and checks through the mail; loading money onto debit cards that the coconspirators registered using the personal identifying information (“PII”) of their victims; purchasing Green Dot MoneyPaks that the coconspirators load onto prepaid debit cards; wiring money through Western Union, MoneyGram, and other electronic money transfer services; and making counter deposits of cash into bank accounts that the coconspirators control.

5. To mask the identity of the scheme originators, the coconspirators use a network of individuals known as “runners.” A runner receives the fraud money, then delivers, mails, or wires the money to another runner or the scheme originator. In return, the scheme originator pays a portion of the fraud proceeds to the runner. This process launders the proceeds of the fraud to conceal the scheme from law enforcement. The use of the runners is generally unknown to the victims. In this case, the coconspirators persuaded the victims that they were sending money to someone associated with a lottery or sweepstakes company, a financial institution, or a federal government agency such as the Internal Revenue Service (“IRS”).

6. **Coconspirator 1** and **Onijah Crighton** (“**Crighton**”) were indicted for their participation in the advance fee lottery scheme. On November 13, 2017, **Coconspirator 1** and **Crighton** were charged with wire and mail fraud conspiracy, in violation of 18 U.S.C. § 1349; and two counts each of wire fraud, in violation of 18 U.S.C. § 1343. On March 21, 2018, **Coconspirator 1** was murdered. **Crighton** subsequently pled guilty to wire fraud conspiracy, and on December 10, 2018, was sentenced to 57 months’ imprisonment.

The Scheme to Defraud PG

7. The investigation partly relates to **BROWN**, **Coconspirator 1**, and **Crighton**’s scheme to defraud Victim PG—an elderly individual with Parkinson’s Disease who resides in Maryland.¹ Starting in April 2013, an individual who identified himself as “Tony Wilson” began contacting PG. Wilson convinced PG that he had won a \$2.5 million lottery prize and that he needed to pay advance fees and taxes to collect that prize.

8. According to records PG kept, PG sent 44 payments worth approximately \$110,000 to Wilson and his runners using Western Union, Green Dot, and express mail. Agents have corroborated the accuracy of PG’s records through bank records, mail receipts, and Western Union records. The investigation ultimately proved that Tony Wilson was **Coconspirator 1** and that **Coconspirator 1** used the alias “Tony Wilson” to mask his identity.

9. By January 2014, PG had reported the fraud to the government and allowed the government to communicate—in an undercover capacity—with Wilson on PG’s behalf. Thereafter, the government set up an undercover email account in PG’s name to communicate with Wilson.

¹ To protect the safety of victims and witnesses, the genders of pronouns have been changed at times throughout this affidavit.

10. By early 2014, Wilson was using the email address samhouston1091@gmail.com to communicate with the undercover agent (who Wilson believed to be PG). Wilson also called and texted PG using a phone number ending in 1206 (the “1206 number”). For instance, on January 20, 2014,² after PG asked Wilson to refund the advance fees he paid, Wilson sent PG the following lulling email from samhouston1091@gmail.com, stating that it would take Wilson months to return PG’s money:

Hi [PG] this is Tony Wilson , on regards of the refunds that’s is available for reimbursement , there is entitlements that needs to be assured due to fact of securing these funds for you over a period of 3months, I really wish you had an phone to communicate with [sic].

11. On January 22, 2014, using samhouston1091@gmail.com, Wilson told PG that PG could still collect his \$2.5 million prize and that Wilson would nonetheless refund a portion of PG’s money:

[PG] I don’t know what imposter you have been dealing with . We have a refund for you of \$56,975. Your merchant banker was located 7744 Normandy rd , hyattsville md. We officially stop speaking at the time you said your son was in critical accident . Your exact and only winnings to two million five hundred thousands dollars 2.5million . Your assigned delivery driver at the time was John terry , we had your check being help at the sterling airport claims department during this time as well, my assistant is ms Valencia [sic].

12. That day, Wilson (using samhouston1091@gmail.com) confirmed for PG that PG had already paid \$109,680, but told PG, “you did not complete your final fee of clearing your prize winnings for your area Exemption tax fee.”

13. On February 19, 2014 (again using samhouston1091@gmail.com), Wilson emailed the undercover PG email account and explained that PG would need to present receipts from his

² All dates in this affidavit are approximations, i.e., are expressed as being “on or about” the date described in the affidavit. Similarly, all amounts are approximations.

payments to collect his prize money, stating, “so far I could make timing for next week , as part of requirements do you have previous receipts ?”

14. The government’s investigation proved that **Coconspirator 1** was the user of samhouston1091@gmail.com. Several of the samhouston1091@gmail.com emails—including emails sent on January 20 (in which the user of samhouston1091@gmail.com identifies himself as Wilson) and January 22, 2014—were sent from the IP address 66.71.5.62 (“the 562 IP address”).³ The 562 IP address traced back to a Penn State University (“PSU”) satellite campus in Altoona, Pennsylvania. On March 11, 2014, agents observed **Coconspirator 1** in Altoona. Agents also used location data from the 1206 number—the number Wilson used to contact PG—to track the phone to Altoona, and observed **Coconspirator 1** in the immediate area of the 1206 phone. When a UC agent posing as PG called the 1206 phone, surveillance agents observed **Coconspirator 1** pull a phone out of his pocket, look at it, and place it back into his pocket. The UC agent advised surveillance agents that the phone call was not answered.

15. Working with officials at PSU, agents discovered that the 562 IP address was assigned to Witness 1, a PSU student who on at least three occasions sent money to **Coconspirator 1** through Western Union. Witness 1 has since informed the government that she was one of **Coconspirator 1**’s runners and received money on **Coconspirator 1**’s behalf as part of the lottery scheme, and admitted to her own involvement in the scheme as late as 2017. Witness 1—who was romantically involved with **Coconspirator 1**—told the government that **BROWN, Crighton**, and **Coconspirator 2** executed the lottery scheme, and that **Coconspirator 3** was the leader of the conspiracy. According to Witness 1, **Coconspirator 3** gave **BROWN, Crighton**, and **Coconspirator 2** directions on how to execute the lottery scheme.

³ The government obtained a search warrant for samhouston1091@gmail.com on February 6, 2018.

16. On February 23, 2014, agents tracked Wilson's 1206 phone to a Budget Inn Hotel in College Park, Maryland. Agents learned that **Coconspirator 1** had checked into the hotel two days earlier using his own name, home address, and passport number, and had paid for both nights in cash. At law enforcement's direction, a hotel employee called **Coconspirator 1**'s room and asked if he was speaking with **Coconspirator 1**. **Coconspirator 1** replied affirmatively. The employee then asked **Coconspirator 1** to stop by the front desk prior to checking out. When **Coconspirator 1** went to the lobby, he stayed for a few moments to check emails on his phone. While he did so, one of the agents looked over **Coconspirator 1**'s shoulder and saw that **Coconspirator 1** was reading emails from an account in PG's name.

17. Upon reviewing records from Western Union and the internet provider for the 562 IP address, the government uncovered additional evidence that **Coconspirator 1** assisted in defrauding PG. On July 25, 2013—at Wilson's direction—PG sent \$1,500 through Western Union payable to **Coconspirator 1**. That day, **Coconspirator 1** withdrew the money from Western Union in Hyattsville using his passport to prove his identity. One day later—once again at Wilson's direction—PG sent \$900 through Western Union to **Coconspirator 1**. This time, **Coconspirator 1** withdrew the money from Western Union using his driver's license to prove his identity. On other occasions, **Coconspirator 1** directed PG to send cash through the mail. Between late April and early July 2013, **Coconspirator 1** convinced PG to send 10 express packages of cash addressed to **Coconspirator 1** (who used a slight variation of his real name) in Hyattsville, Maryland.

18. With respect to evidence obtained from IP records, the government learned that **Coconspirator 1** also used the 562 IP address to log onto his own Facebook account. In fact, on at least one occasion, **Coconspirator 1** logged onto his Facebook account from the 562 IP address

the day he sent an email from samhouston1091@gmail.com using the 562 IP address. Thus, the evidence showed that **Coconspirator 1** assisted in the scheme to defraud PG, leading to his federal indictment in October 2017.

Onijah Crighton's Participation in the Lottery Scheme

19. Between November 19, 2013 and December 19, 2013, the user of the email account hotskullz@gmail.com sent PG approximately 21 emails. The emails purported to confirm that PG won a prize and continued to solicit money from PG. For instance, on November 19, 2013, hotskullz@gmail.com sent an email to PG. The email, which was addressed to PG and contained PG's home address, stated in part:

Dear [PG],

The team at PCH is pleased to officially announce your name as the second place winner of the 10 Million Dollars (\$10,000,000) Grand Prize Draw, sponsored by Reader's Digest Magazine. The total amount being claimed for second place is Ten Million U.S. dollars (\$10,000,000), Congratulations! The Publisher Clearing House will make all necessary arrangements in order for you to receive your prize.

The email was signed "Congratulations again, Tony Williams Chief Financial Officer."

20. On December 9, 2013, hotskullz@gmail.com emailed PG a message that stated in part, "Okay [PG] . . . I tried to contact you because the (IRS) is on my ass right now. LOL But thank you for emailing me to let me know at's [sic] going on[.] am [sic] going to inform them about the situation so they can give you till tomorrow be in touch." The email was signed "Tony."

21. On December 11, 2013, hotskullz@gmail.com emailed PG stating, "Hi [PG], It's tony [sic] I was wondering how the weather & you doing now and if it's possible for you to make the payment tomorrow. If so you going to send it to the address: 308 70th place [sic] Capital heights [sic] MD 20743 to [Witness 7] & remember to send it in the express mail also please give me a call before you do anything okay, because I want for you to receive your delivery no later then

[sic] Friday.” Records show that the email was sent from an Apple iPhone that was connected to the internet while using the IP address 69.250.43.133 (“the 133 IP address”).

22. During the investigation, the government obtained evidence proving that **Crighton** used the hotskullz@gmail.com email address to send the fraudulent emails to PG and other victims of the lottery scheme. First, records obtained from Apple reflect that the email address hotskullz@gmail.com was used in February 2012 to register an Apple account with the Apple ID hotskullz@gmail.com.⁴ As part of the Apple ID registration process, Apple requires users to provide personal identifying information. When creating the Apple ID hotskullz@gmail.com in 2012, the registrant provided the name “**Onijah Crighton**” and a physical address on Reicher Street in Hyattsville, Maryland (“the Reicher Street address”), the address where **Crighton**’s parents resided. And on January 4, 2013, **Crighton** was issued a Maryland Driver’s license that listed his home address as the Reicher Street address.

23. Further, some of the IP addresses that the hotskullz@gmail.com email account used while sending emails to PG were also used to access other online accounts associated with **Crighton**. For example, on December 11, 2013—the date that hotskullz@gmail.com sent an email to PG from the 133 IP address—**Crighton** accessed his Facebook account from the 133 IP address.

24. Witness 2—who was close acquaintances with **Crighton**—told agents that he sat next to **Crighton** while **Crighton** used the email account hotskullz@gmail.com. Witness 2 also listened to recorded conversations between PG and individuals associated with the lottery scheme and identified **Crighton**’s voice on more than one of those recordings.

25. Remotely stored in the hotskullz@gmail.com account, agents found **Crighton**’s school homework and bank records for an account over which **Crighton** had signatory authority.

⁴ The government obtained a search warrant for hotskullz@gmail.com on December 12, 2013.

Further, in the hotskullz@gmail.com account, agents discovered PII (including names, social security numbers, telephone numbers, and home addresses) that belonged to elderly individuals, including PG.

Keno Brown

26. On December 11, 2013, **Crighton** sent an email from hotskullz@gmail.com to PG that requested an additional payment that PG had to make to collect his prize. An undercover agent replied to **Crighton**, telling him that a debit card would be sent to him that he could use to withdraw money for the fees associated with the prize.

27. On December 13, 2013, the government made a controlled delivery of a debit card in PG's name to 308 70th Place, Capitol Heights, Maryland 20743. An undercover agent delivered the package to two males, one of whom was immediately identified as **Crighton**. Agents conducting surveillance later identified the second male as **BROWN**. After accepting delivery for the debit card, **Crighton** and **BROWN** got in a car and drove away from 308 70th Place, Capitol Heights, Maryland.

28. As **BROWN** and **Crighton** drove away, the passenger of the vehicle—who was identified as **BROWN**—threw the envelope and a white piece of paper out of the passenger side window. The torn envelope and piece of paper were collected as evidence and submitted to the USPIS Forensic Laboratory for examination. A latent fingerprint found on the piece of white paper was positively identified as **BROWN**'s fingerprint.

29. That day, video surveillance from an Exxon Mobile station located at 5650 Annapolis Road, Bladensburg, Maryland, showed **Crighton** and **BROWN** entering the Exxon station together. **Crighton** attempted to withdraw money from an ATM inside the station using the debit card in PG's name. At the time of his arrest for the instant offense, **Crighton** admitted to

receiving this debit card, and during the execution of a federal search warrant on May 11, 2018, **BROWN** admitted that he was depicted in the Exxon surveillance footage.

Witness 3

30. In May 2018, the government interviewed Witness 3, who told the government that **BROWN** is the father of her child. Records from Bank of America show that between May and June 2017, Witness 3's bank account had seven counter deposits totaling approximately \$10,950. Those deposits were made in Oregon, California, New Mexico, Oklahoma, and North Carolina. One of the deposits was from an individual with the initials BK who resided in California and was born in 1922.

31. Witness 3 told the government that she gave the debit card for this Bank of America account to **BROWN**, who was the one who used the account. Witness 3 did not know who made the counter deposits, nor did she know why those individuals made those deposits. When Witness 3 asked **BROWN** why he wanted to use her debit card, **BROWN** told Witness 3 that he wanted to buy groceries and improve her credit.

Witness 6

32. On numerous occasions during the investigation, the government interviewed Witness 6, who was romantically involved with **BROWN**. In January 2018, **BROWN** and Witness 6 had a child together. During the investigation, Witness 6 told the government that she overheard **BROWN** using a "flip phone" to tell someone that he won a \$2 million sweepstakes. When Witness 6 asked **BROWN** what the conversation was about, **BROWN** responded, "mind your business."

33. Records from MoneyGram and RIA Financial show that between 2013 and early 2016, Witness 6 received numerous electronic money transfers from individuals located

throughout the United States who are senior citizens. Witness 6 told the government that acting on **BROWN**'s directions, Witness 6 gave the money from the electronic transfers to **BROWN**.

Witness 7

34. In May 2018, Witness 7—who met **Crighton** in 2012 and was romantically involved with **Crighton**—told the government that **Crighton** had approximately 60 debit cards in other individuals' names sent to her residence.⁵ According to Witness 7, she did not recognize the names on the cards. When Witness 7 questioned **Crighton** about the cards, **Crighton** told her to “mind her own business.” According to Witness 7, she gave at least some of the debit cards to **BROWN**.

35. Witness 7 also explained that **BROWN** and **Crighton** were friends, and that on numerous occasions, **BROWN** directed Witness 7 to send money through and pick up money from Western Union. Further, on one occasion, Witness 7 overheard **BROWN** on the phone talking about a sweepstakes and telling someone to send money.

Witness 8

36. In July 2018, the government interviewed Witness 8, who met **BROWN** approximately five years ago and was romantically involved with **BROWN**. The first time she met **BROWN**, she “smoked” with **BROWN** and **Crighton**. According to Witness 8, while she and **BROWN** were dating, **BROWN** participated in a lottery scheme with **Crighton** and several other individuals.

37. Witness 8 learned that **BROWN** was involved in the lottery scheme while living in an apartment with **BROWN** (that according to Witness 8 was located on Toledo Terrace). During

⁵ Records from RushCard show that debit cards opened using the identities of elderly individuals were sent to Witness 7's residence as far back as May 2013. Witness 7 stated that she had not spoken to **Crighton** in two to three years.

that time, Witness 8 heard **BROWN** on the phone—talking in a “female” voice—telling someone that he won a lottery prize and needed to pay fees to collect the prize. Witness 8 overheard **BROWN** making lottery scheme calls on approximately five occasions. Witness 8 also overheard **BROWN** on the phone telling people to purchase Green Dot cards on several occasions. Further, Witness 8 told the government that **BROWN** had an iPhone and a “flip phone,” and that **BROWN** used the flip phone for the lottery scheme.

Witness 9

38. Witness 9 has known **Crighton** and **BROWN** for approximately eight years. According to Witness 9, Coconspirator 3 taught **BROWN** and **Crighton** how to execute a lottery scheme and instructed them to change their voices on the phone when making fraudulent phone calls to victims. According to Witness 9, he heard both **BROWN** and **Crighton** talking on the phone in an altered voice.

Victim NE

39. On March 5, 2018, the government interviewed Victim NE, a senior citizen living in Colorado Springs, Colorado. According to NE, a man who said he was a representative of a lottery or sweepstakes recently told NE that NE was required to pay taxes to receive a \$5.4 million prize. NE recalled sending several packages through the mail that contained either cash or checks (or both) in order to receive his prize. NE recalled sending those packages to Hyattsville.

40. Records from FedEx show that NE sent approximately nine packages addressed to either **BROWN** or Witness 3, who was romantically involved and had a child with **BROWN**. For example, on December 1, December 20, December 30, 2017, and January 16, 2018, NE sent FedEx packages from Colorado Springs to Witness 3 at 3417 Toledo Terrace, Apartment B1, Hyattsville, Maryland 20782 (“the Toledo Terrace address”).

41. When agents showed Witness 3 a photograph of the complex where the Toledo Terrace address is located, Witness 3 identified the complex as where **BROWN** resides and described **BROWN**'s unit in a way that was consistent with Apartment B1 of the Toledo Terrace address. According to Witness 3, **BROWN** resides at the Toledo Terrace address with his mother. Leasing records for the Toledo Terrace address show that the address is leased to **BROWN**'s mother.

42. On December 23, 2016, **BROWN** submitted a form with the United States Postal Service to change his address from 5802 Annapolis Road, Apartment 408, Bladensburg, Maryland 20710 ("5802 Annapolis Road") to the Toledo Terrace address. Records from the United States Postal Service show that **BROWN** recently received mail at the Toledo Terrace address. Further, on May 11, 2018, the government executed a federal search warrant on the Toledo Terrace address and encountered **BROWN** living in one of the bedrooms.

43. Of the nine packages that NE sent to **BROWN** or Witness 3, four of the packages went to 5802 Annapolis Road between July 26, 2016 and August 4, 2016 and were addressed to either **BROWN** or "reno brown."

44. Witness 3 told agents that **BROWN** called one morning to tell her that a package would be delivered to her home in Brentwood, Maryland, and that the package was for **BROWN**. **BROWN** instructed Witness 3 to hold the package until he picked it up. After the package was delivered, Witness 3 saw that it was from Colorado Springs, Colorado.

45. Records from RIA Financial show that on at least three occasions between April 2015 and February 2016, NE made electronic money transfers to **BROWN** and Witness 6 for amounts greater than \$500.

Victim LS

46. On March 8, 2018, the government interviewed Victim LS, who is a senior citizen living in Oklahoma. Starting in early 2017, LS was told that she won a prize and needed to pay fees to collect the prize. To pay the fees, LS sent personal checks and cashier's checks through the mail. LS cashed out multiple life insurance policies to pay for the fictitious fees and ultimately lost her life savings. LS remembered sending at least \$86,000 in checks to receive her prize.

47. LS kept documents associated with her payments. One of those documents was a \$1,000 cashier's check that LS purchased on May 30, 2017 from Arvest Bank that was payable to Witness 3. Records from Bank of America also show that on May 31 and June 1, 2017, counter deposits of \$1,400 and \$4,500 were made into Witness 3's bank account. The branch where the deposits were made is located in Oklahoma City, Oklahoma, near LS's residence.

Victim ES

48. On November 27, 2018, the government interviewed Victim ES, who is a senior citizen living in Florida. ES received a call from a man who said he worked for Publishers Clearing House. That man told her that she needed to pay fees to receive a multimillion dollar prize and a Mercedes Benz. ES recalled purchasing money orders and sending them to Maryland. Records from RIA Financial show that between November and December 2015, ES sent five electronic money transfers totaling \$1,918 from a Walmart in Florida to **BROWN** in Maryland.

Victim ER

49. On November 26, 2018, the government interviewed Victim ER, who is a senior citizen living in Florida. ER received a call from someone who worked for Publishers Clearing House. That person told ER that she won a prize worth millions of dollars. ER recalled sending money through Walmart to receive her prize, but did not recall how many times she sent money.

Records from RIA Financial show that on January 1, 2017, ER sent \$500 to Witness 3, who told the government that **BROWN** had her receive money transfers at Walmart and thereafter provided that money to **BROWN**.

Victim JH

50. On November 26, 2018, the government interviewed Victim JH, who is a senior citizen. JH was told that she won an \$8.9 million prize. Over several months, JH sent money through Walmart and Western Union to collect her prize. JH also remembers that she deposited fees for her prize into a Bank of America account located in Redmond, Oregon. On June 7, 2017, Witness 3 received a counter deposit of \$3,000 into her Bank of America account at a branch in Redmond, Oregon. Witness 3 informed the government that during this time, **BROWN** used her debit card and had access to the account that received the \$3,000 counter deposit.

Victim ST

51. On November 27, 2017, the government interviewed Victim ST, who is a senior citizen living in California. In 2015, someone who identified himself as “Ben Wilson” called ST to tell her that she won a \$3.5 million prize and a Mercedes Benz. For several months, ST paid taxes and storages fees to collect her prize. To pay the fees, ST purchased money orders and mailed them to people in Maryland and New York. ST also sent money through MoneyGram, Western Union, and Walmart. ST remembered sending money to Hyattsville, Maryland. ST had to borrow money from her Individual Retirement Account to pay for the prize, and estimates that she lost between \$10,000 and \$100,000. The financial harm to ST had a significant impact on her financial stability.

52. ST specifically remembered sending money to **BROWN** to receive her prize. ST recalled this name because it was unique. Records from RIA Financial show that ST sent a \$250

electronic money transfer to **BROWN** in April 2015. ST also recalled sending money by placing \$100 bills between the pages of magazines that she then mailed, though ST could not remember exactly where she mailed the money.

Victim TC

53. On November 26, 2018, the government interviewed Victim TC, who is a senior citizen living in California. TC received a phone call from someone who said he worked for Publishers Clearing House. This person told TC that he won a prize valued at \$1,000, but was required to pay \$100 to collect his prize. TC went to Walmart to pay the fee. After making the payment, TC realized that the prize was not real. Records from RIA Financial show that on February 13, 2016, TC wired \$100 to **BROWN**.

Victim MM

54. On July 30, 2018, the government interviewed Victim MM, who is a senior citizen living in Indiana. MM told the government that several people called to tell her that she won a \$500 million prize through Publishers Clearing House. To receive her prize, MM sent approximately \$20,000 through Western Union, MoneyGram, and Walmart. MM recalled sending money to Hyattsville.

55. Records from RIA Financial show that in June 2017, MM sent \$440 to Witness 3, who informed the government that **BROWN** had people send money to her through Walmart and further directed her to withdraw the money from Walmart and give the money to **BROWN**. According to contemporaneous handwritten notes that MM kept, MM mailed a package containing money to Witness 3 at the Toledo Terrace address where **BROWN** lives with his mother.

Victim DV

56. On August 28, 2018, the government interviewed Victim DV, who is a senior citizen living in Iowa. DV received a call from an individual who said he worked with Publishers Clearing House, and who told DV that he won a prize valued at millions of dollars and a car. According to DV, he paid approximately \$60,000 in fees to collect his lottery prize.

57. Records from MoneyGram show that on July 10, 2013, DV sent \$1,500 to Witness 6—the mother of one of **BROWN**'s children—who withdrew the money in Maryland. Records from MoneyGram also show that on July 12, 2013, DV sent \$2,800 to Witness 2 (**Crighton**'s former girlfriend).

Victim CW

58. On November 26, 2018, the government interviewed Victim CW, who is a senior citizen living in Georgia. CW received a call from a man who said he worked for Publishers Clearing House and that CW had won a multimillion dollar prize and a car. CW recalled paying fees through Western Union to Witness 6 to receive her prize. Records from MoneyGram show that in June and July 2014, CW sent \$2,350 to Witness 6 in Maryland.

Victim MB

59. On December 3, 2018, the government interviewed Victim MB, who is a senior citizen living in North Carolina. MB received a call from someone who said he worked for Publishers Clearing House and that MB won a multimillion dollar prize and a Mercedes Benz. MB recalled sending approximately \$10,000 in personal money orders to obtain her prize. Records from RIA Financial show that on July 26, 2017, MB sent a \$390 money transfer to Witness 3 in Maryland.

The Source of the Conspiracy's Victims

60. **BROWN, Crighton, and Coconspirator 1** conspired to defraud over 100 elderly victims. To identify target victims, **BROWN, Crighton, and Coconspirator 1** purchased what are known as “lead lists,” which are lists of names, addresses, phone numbers, and other PII belonging to elderly individuals who **BROWN, Crighton, and Coconspirator 1** targeted.

61. For instance, the government obtained evidence that **Coconspirator 1** used Yahoo Account 1 to purchase lead lists over the internet.⁶ Records from Yahoo show that in December 2015, Yahoo Account 1 exchanged an email with internationaldataproducs@gmail.com. That email account belonged to **Cooperating Defendant 1**, who pled guilty to one count of wire fraud in the Middle District of Florida and admitted to selling lead lists over the internet.⁷ In 2018, the government obtained records from **Cooperating Defendant 1** (who produced those records as part of his cooperation agreement) showing that in August 2013 and December 2015, using samhouston1091@gmail.com, **Coconspirator 1** emailed **Cooperating Defendant 1** to purchase a lead list.

62. Similarly, emails from **Cooperating Defendant 1** show that **Crighton** used hotskullz@gmail.com to purchase lead lists from **Cooperating Defendant 1**. For example, in August 2013, **Crighton** (using hotskullz@gmail.com, which displayed a signature name of “Onijah”) emailed **Cooperating Defendant 1**, “I need some good work I wanna make some money I need some fresh data base & coupom just contact me ASAP at hotskullz@gmail.com with your prices [sic].”

⁶ **Coconspirator 1**'s Facebook account was registered with Yahoo Account 1. Further, this email address comprised **Coconspirator 1**'s initials and his year of birth.

⁷ The government obtained a search warrant for Yahoo Account 1 on February 16, 2018.

63. Records from Apple show that Apple ID longlife1965@gmail.com used the iCloud backup feature to store photographs taken with an Apple device. Some of the photographs from this Apple account depict **BROWN**. **BROWN** has the words “long” and “life” tattooed on his hands, and his mother confirmed that he uses the email address longlife1965@gmail.com. Further, on an immigration application for naturalization, **BROWN** reported that his email address was longlife1965@gmail.com. Finally, according to records from Google, longlife1965@gmail.com was registered using **BROWN**’s cell phone number (a number ending in 9472).

64. Pursuant to federal search warrants, the government obtained communications between hotskullz@gmail.com (**Crighton**’s email address) and longlife1965@gmail.com that show that **Crighton** forwarded lead lists from hotskullz@gmail.com to longlife1965@gmail.com. For instance, on May 28, 2013, longlife1965@gmail.com sent an email to hotskullz@gmail.com with the subject line “Fwd: 105 DATABASE AND 36 COUPONS.” The email had 13 attachments, including one spreadsheet and 12 photographs. The spreadsheet was a list of more than 100 names, addresses, phone numbers, and ages that ranged from 60 to 87 years old.

65. Similarly, on June 7, 2013, longlife1965@gmail.com sent an email to hotskullz@gmail.com with the subject line “Fwd: 383 NAMES.” Attached to the email was a spreadsheet cataloguing approximately 384 names, addresses, phone numbers, and ages. The ages ranged from 60 to 77 years. On December 9, 2013, hotskullz@gmail.com sent an email to longlife1965@gmail.com attaching a 20-page document containing the names and contact information of numerous individuals.⁸

⁸ Records from Google show that longlife1965@gmail.com was accessed on a computer that also accessed americanlotto286@gmail.com. The name of this email account suggests **BROWN**’s involvement in the lottery scheme.

Conspiracy to Commit Access Device Fraud

66. When a debit card or prepaid debit card account is opened, financial institutions, such as RushCard, Green Dot, and AccountNow, send the physical debit card to the address provided on the account application. Those financial institutions normally send client notifications to the email address or phone number identified on the application for the debit card.

67. Using various emails accounts—including `longlife1965@gmail.com`, [Victim BR]@yahoo.com, and `kenobrown17@yahoo.com`—**BROWN** used his phone number (the number ending in 9472) and the PII of senior citizens to fraudulently apply for RushCards. **BROWN** also used his 9472 phone number, the street address 3501 Toledo Terrace, and the email address [Victim BR]@yahoo.com to register a RushCard in his own name.⁹

68. For instance, records from RushCard show that between February and August 2013, at least nine applications for debit card accounts were submitted with the email address `longlife1965@gmail.com` using the PII of individuals who had no apparent connection to **BROWN**. In some cases, the government interviewed the victims, who did not know debit cards were enrolled using their identities. The individuals whose identities were used to open those debit cards were born in the 1920s, 1930s, and 1940s.

69. Several of the RushCard applications described in the previous paragraph were submitted between February and July 2013 from IP address 98.204.174.113 (“the 4113 IP address”). Records show that between January 2013 and January 2014, there were numerous logins

⁹ On July 12, 2012, the email address `kenobrown17@yahoo.com` was created using the IP address 68.50.173.144 (“the 144 IP address”). Yahoo records show that this email account is registered to **BROWN**. That day, **BROWN**’s personal Facebook account was activated online under the handle “Grimrim Bwoy” and using the 144 IP address. On November 12, 2012, **BROWN** used the email address `kenobrown17@yahoo.com` to sign up for an Apple account in his own name. **BROWN** opened this account online using IP address 172.56.3.226 (“the 226 IP address”) that was registered to **BROWN**’s residence on Toledo Terrace in Hyattsville, Maryland.

from the 4113 IP address to **BROWN**'s Facebook account, **Crighton**'s Facebook account, and hotskullz@gmail.com account.

70. The following are additional examples of **BROWN** using the PII of elderly individuals to commit access device fraud:

- a. Using the PII of Victim LK (who was born in 1927), **BROWN** enrolled several RushCards under the email address longlife1965@gmail.com. On September 26, 2017, the government interviewed LK, who previously had been told that she won a \$2.5 million lottery prize. According to LK, she spent approximately \$100,000 to collect her lottery prize, at times by purchasing Green Dot MoneyPaks at CVS stores and sending cash through the mail. LK did not know that there were RushCards in her name.
- b. Records from Green Dot show that a debit card was activated on October 24, 2012 using the PII of Victim BR, a senior citizen who resided in California. The account was registered to the email address kenobrown17@yahoo.com and mailing address 3501 Toledo Terrace L4, Hyattsville, Maryland 20782, which is **BROWN**'s former address before **BROWN** and his family moved to Apartment B1 at 3417 Toledo Terrace in November 2016.¹⁰
- c. Records from Bancorp indicate that in 2013, a prepaid debit card was enrolled using the PII of Victim HW. The card was registered to **BROWN**'s address on Toledo Terrace in Hyattsville, Maryland, along with the email address kenobrown17@yahoo.com. Records show that the card was used in Maryland. A review of the transaction history for the debit card showed that several transactions were conducted in Maryland, including transactions in Hyattsville, Bladensburg, Riverdale, Landover Hill, and Takoma Park. When interviewed, HW did not recall traveling to Maryland, opening a RushCard, or giving anyone permission to open a prepaid debit card using his PII. HW also told agents that he was the victim of a lottery scheme. HW told agents that in order to obtain his prize, he made approximately 100 payments.
- d. On February 7, 2013, a RushCard application was submitted online using the PII of Victim NS and the IP address 98.204.174.113 ("the 113 IP address"). The application reflects an address in Maryland, **BROWN**'s phone number (ending in 9472), and the email address [Victim BR]@yahoo.com. Facebook records show on February 8, 2018, **BROWN** logged into his Facebook account twice using the 113 IP address. Over the next four days, two additional RushCard and Green Dot

¹⁰ Records from Western Union show that between April 2011 through June 2012, BR sent **BROWN** approximately 34 money transfers totaling approximately \$4,560. Records from MoneyGram show that in February 2016, BR sent one money transfer to **BROWN** for approximately \$70.

applications were submitted using NS's PII, one of which was from the 113 IP address. On February 11, 2013, **BROWN** accessed his Facebook account two more times from the 113 IP address.

- e. On February 12, 2013, two Green Dot cards were enrolled using the PII of Victim MF. The applications reflect **BROWN**'s address on Toledo Terrace as the registrant address, along with the email address [Victim BR]@yahoo.com.
- f. Between September 18 and September 20, 2013, four Green Dot cards were enrolled using the PII of Victim PU. The address provided on the applications for two of those cards was **BROWN**'s residence on Toledo Terrace in Hyattsville, Maryland. The address provided on the other two Green Dot card applications was the address where Witness 6 (the mother of **BROWN**'s child) resided in Rapidan, Virginia. All four debit cards were registered using the email address [Victim BR]@yahoo.com.

71. **BROWN** also used Witness 6's email address and physical address to fraudulently obtain debit cards (to reiterate, Witness 6 is the mother of one of **BROWN**'s children). Google subscriber records show that Gmail Account 1 (which comprises Witness 6's first initial and last name) is registered to Witness 6. Records from RushCard show that between May 2013 and June 2014, 18 applications for debit card accounts were submitted with Gmail Account 1 using the PII of individuals who were born between 1920 and 1961.

72. In May 2018, Witness 6 told the government that, with one exception, she did not know the individuals whose PII was used to open the RushCards with her email account. Notably, Witness 6 informed the government that **BROWN** had the password to and used her email account. Further, Witness 6 told the government that several years ago, **BROWN** had hundreds of debit cards from RushCard, Green Dot, and AccountNow sent to her residence on Constitution Highway in Rapidan, Virginia.¹¹ According to Witness 6, **BROWN** directed her to hold the debit cards until

¹¹ Records from Apple show that **BROWN** used the instant messaging application WhatsApp and the email account longlife1965@gmail.com. On April 9, 2014, **BROWN** exchanged a WhatsApp message with an unknown individual who provided the name of Victim SM, who was born in 1926. The message also contained SM's date of birth, social security number, driver's license number, mother's maiden name, and address, and stated, "Sen to [Witness 6's address] constitution hwy rapidan VA22733 [sic]."

he could pick them up, and if she failed to comply with his directions, **BROWN** physically abused Witness 6.

Brown's Digital Notes and Google Search History

73. During the investigation, Apple produced documents that were responsive to federal search warrants executed on the Apple accounts `hotskullz@gmail.com` and `longlife1965@gmail.com`. Those records showed that **BROWN**—using the Apple ID `longlife1965@gmail.com`—created the following digital notes.

- a. “[Victim MM]” on June 5, 2017. To reiterate, Victim MM was the lottery scheme victim who sent money to Witness 3 and to **BROWN**'s residence on Toledo Terrace in Hyattsville, Maryland.
- b. “828286-3874” on July 7, 2017. According to Victim MB, the individual who told her she won a lottery prize contacted her from this phone number.

74. In May 2018, Google produced documents that were responsive to a federal search warrant executed on `longlife1965@gmail.com`, including Google internet search records for `longlife1965@gmail.com`. Those records showed that **BROWN** conducted the following Google searches:

- a. “publisher clearing” on September 10, 2014.
- b. “andy goldberg from pch” on September 10, 2014. Andy Goldberg is the Chairman and CEO of Publishers Clearing House.
- c. “moneypak” on September 5, 2014.
- d. “what’s a telemarketing script” on November 27, 2013.
- e. “a letter from the IRS informing a person about their mega millions winners” on November 20, 2013.
- f. “a letter from the IRS informing a person about their latroy winnis [sic]” on November 20, 2013. Notably, that day, Victim PG received an email with an attachment that was a letter to PG bearing the IRS insignia and notifying PG that he won a \$10 million prize from Publishers Clearing House and was required to

pay a “re-leasing” fee of \$5,000. The letter also directed PG to contact a man named “Henry Washington” at a number ending in 6256. **BROWN** used this phone number to send MoneyGram and Western Union transfers. **BROWN** also used this phone number—along with the email address longlife1965@gmail.com—to enroll three PayPal accounts in other individuals’ names (including the names of **BROWN**’s mother, Witness 6, and a woman living in Prescott, Arizona who was born in 1960).

- g. “american dreams sweepstakes” on November 19, 2013.
- h. “sweepstakes leads broker” on November 19, 2013.
- i. “mega millions account number for sale” on November 19, 2013.
- j. “official letter from the mega millions” on November 19, 2013.
- k. “a official letter from the publisher clearing house” on November 19, 2013.
- l. “mega millions calling number” on November 19, 2013.
- m. “prepaid debit cards” on May 26, 2013.

75. Google records also show that **BROWN** engaged in the following internet activity while logged into longlife1965@gmail.com:

- a. On November 19, 2013, **BROWN** went to the website www.freshlotteryleads.com. This websites describes its service as follows: “We have the real leads at the best prices. All of our First Hit Leads are ten to 15 days old, these are the freshest leads you will find. We offer Sweepstakes Leads for both USA and Canada. Our leads are perfect for telemarketers who are looking to increase their sales, find new business, and increase revenue.”

76. Google also produced emails sent and received from the Gmail account longlife1965@gmail.com. On August 26, 2013, from longlife1965@gmail.com, **BROWN** sent an email to rfq@cardusa.com (an email address associated with the debit card manufacturer Card USA). The email read, “MY name is [Victim BR] my card close with some cash and I would like to know hw I go abt getting my cash?” To reiterate, Victim BR is an elderly citizen from the West Coast. Between April 2011 and June 2012, BR sent 34 Western Union transfers totaling \$4,560 to **BROWN**. MoneyGram records show that BR sent an additional money transfer to **BROWN** in

February 2016. Further, when registering kenobrown17@yahoo.com, **BROWN** provided a phone number ending in 7687. Toll records show that in 2013, the 7687 number had over 100 phone contacts with BR.

77. Between October 2011 and September 2013, **BROWN** opened numerous debit cards using BR's PII and assumed BR's identity to create the email address [Victim BR]@yahoo.com, which **BROWN** then used to fraudulently enroll additional debit cards. Thus, based on training, experience, and knowledge of the investigation, I believe that when **BROWN** sent the foregoing email to Card USA, he was asking Card USA how he could retrieve the fraud proceeds on the debit card that he enrolled using BR's identity.

Search Warrant on Toledo Terrace

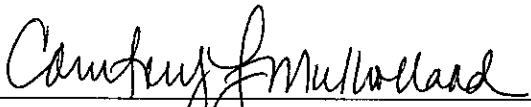
78. On May 11, 2018, the government executed federal search warrants on two residences, one of which was 3417 Toledo Terrace Apartment B1, Hyattsville, Maryland—the residence where **BROWN** and his mother resided. During the search, agents encountered **BROWN**, and recovered multiple flip phones and printed lead lists that bore handwritten notes. Agents also recovered a laptop in **BROWN**'s bedroom. That device contained three lead lists (one PDF and two Excel spreadsheets). The PDF was eight pages long, and the two Excel files contained the PII of approximately 800 individuals. The years of birth on the various lead lists found in **BROWN**'s possession ranged from 1913 to 1946.

79. During the execution of the search warrant, agents conducted a Mirandized interview of **BROWN**. When questioned about the email address longlife1965@gmail.com, **BROWN** denied that the email address was his and represented to agents that longlife1965@gmail.com was his mother's email account. An agent thereafter photographed the words "long" and "life," which were tattooed on **BROWN**'s hands.

80. Because the investigation was ongoing, **BROWN** was not arrested at the time of the execution of the search warrant.

CONCLUSION

81. Based on the foregoing facts, there is probable cause to support the issuance of the requested warrant.



Courtney L. Mutholland
United States Postal Inspector

Subscribed and sworn to before me on January 2, 2019.



The Honorable Gina L. Simms
United States Magistrate Judge