FILED

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

2016 SEP 28 PM 4:29

2:16-cr-109-FtM-29CM

UNITED STATES OF AMERICA

Case No. _____

v.

RONALD JOHN MENDLESKI

18 U.S.C. § 2
18 U.S.C. § 1343
18 U.S.C. § 1349
18 U.S.C. § 982 [Forfeiture]
28 U.S.C. § 2461(c) [Forfeiture]

INDICTMENT

The Grand Jury charges:

BACKGROUND

At all times relevant to this Indictment, unless otherwise indicated:

Introduction

1. Telemarketers needed access to the contact information of individuals who were willing to listen to their pitch to sell products by phone. The telemarketers' demand for fresh names gave rise to an industry of brokers who collected the contact information of individuals from all over the United States and other countries to sell to businesses pitching products by phone.

2. The personal information that these individuals provided to telemarketers—usually name, phone number, and address—was called a "lead."

3. The people who compiled and sold this information were called "lead brokers."

4. One type of lead that lead brokers sold to telemarketers was called the "sweepstakes lead." Sweepstakes leads were generated from mass mailings that

advertised huge winnings in sham lotteries or prize drawings. To originate these leads, individuals and small companies mass mailed documents notifying the recipients that they had won, or were likely to win, expensive prizes and enormous cash payouts.

5. In order to claim the putative prize, the recipient was asked to mail in an attached slip of paper, on which the recipient was required to list various personal information, such as a name, phone number, and address. These slips of paper were known as "hard copy leads" or "coupon leads." The hard copy leads were then generally sold to lead brokers, who, in turn, provided them to telemarketers with whom the brokers had a business relationship.

6. Additionally, lead brokers regularly bought spreadsheets in which the personal information derived from a group of recent hard copy leads had been compiled. These spreadsheets were called "database leads" or "lead lists." Because these spreadsheets contained the same personal information as the hard copy leads themselves, they were likewise valuable to telemarketers.

7. Many lead brokers, recognizing the prevalence of fraud in parts of the telemarketing industry, took steps to make sure that their clients did not use leads to commit fraud. Some common compliance techniques included verifying a telemarketer's business information, ensuring that the telemarketer had a legitimate website, asking for a copy of the telemarketing script the client planned to use, and having the telemarketers sign legal agreements.

8. Defendant RONALD JOHN MENDLESKI was a lead broker with a principal place of business in Lee County, Florida. MENDLESKI specialized in selling

sweepstakes leads. He regularly sold both hard copy leads and database leads to his clients, who were principally telemarketers.

9. MENDLESKI operated under a variety of business names, including Florida International Data Products, Florida Data International Products, LLC, eData Solutions, iMarketing Leads, and Ron Mendleski Enterprises, LLC, among others. Regardless of the name, the business structure remained unchanged: MENDLESKI was the sole employee and operator of the enterprise, and the business existed principally to sell leads to telemarketers.

10. Co-Conspirator A was a telemarketer who operated a fraudulent telemarketing company in Costa Rica and targeted victims in the United States, among other places.

11. Co-Conspirator B was a telemarketer who operated a fraudulent telemarketing company in Costa Rica and targeted victims in the United States, among other places.

12. Co-Conspirator C was a lead broker who worked with a telemarketer based in Jamaica and targeted victims in the United States, among other places.

Overview of the Fraudulent Scheme

13. From at least in or about January 2009 until at least in or about December 2014, MENDLESKI sold the personal information of tens of thousands of individuals to telemarketers knowing that the telemarketers intended to use those leads to commit fraud.

14. MENDLESKI provided hard copy and database leads to dozens of clients using various means of wire communication. The vast majority of his clients were based

in foreign countries. Most operated from Costa Rica, Jamaica and other locations known to MENDLESKI to be hotbeds for telemarketing fraud.

15. Clients sent MENDLESKI scripts that were on their face fraudulent schemes. For instance, in some of these scripts, the telemarketer claimed that the recipient of the call had won vast sums of money in a spurious sweepstakes, which, because MENDLESKI had provided the lead in the first place, MENDLESKI knew the victims had never even entered.

16. Occasionally, the scripts provided by his clients involved telemarketers posing as a representative of a government entity or legitimate private business when calling potential victims, when MENDLESKI knew that his clients had no actual government or lawful business affiliation.

17. As one example, Co-Conspirator A told MENDLESKI that his pitch to clients was "FTC bla bla etc we pitch winnings of $250k." Co-Conspirator A then sent MENDLESKI a script in which the caller claims the he is a representative of the "Federal Gaming Council" and states that the victim has won $250,000 in a sweepstakes.

18. A former business partner of MENDLESKI's advised MENDLESKI that the script from Co-Conspirator A was "for sure illegal" and "a total scam in plain writing." Nonetheless, several months later, MENDLESKI began selling lead lists to Co-Conspirator A.

19. Some of MENDLESKI's clients explicitly told him about their fraud. For example, Co-Conspirator B, after being asked by MENDLESKI to provide a legal agreement certifying that he was not engaged in fraud and a draft "script," wrote MENDLESKI, "look somewhere else if you want all that info." Co-Conspirator B then

told MENDLESKI "let's be real about it, we both know what we do with the leads... NO BODY calls them for something good and real, so all the customers that have sent you their scripts from [Costa Rica]... are all banging the customers over the head..." Co-Conspirator B then informed MENDLESKI that "if I send you a script we both know is gonna be fake, so save my time and take my order please..." Soon thereafter, MENDLESKI sold Co-Conspirator B thousands of leads. When MENDLESKI later attempted to visit Co-Conspirator B in Costa Rica, Co-Conspirator B declined the invitation, writing MENDLESKI that "[y]ou know Ron, here in Costa Rica everyone knows each other in this industry... And what we do is wrong... Really wrong... And I think you know and you're just playing blind :)". Just days later, MENDLESKI sold Co-Conspirator B additional leads.

20. Many of MENDLESKI's clients lacked any indicators to suggest that they were affiliated with an honest business. For instance, some signed their emails with names that did not match the name to which the email account was registered. Very few of his clients used business email accounts. Only a small number provided any description of their business model.

21. As another example, Co-Conspirator C used a name in his emails to MENDLESKI that was completely different than his email address. Co-Conspirator C told MENDLESKI that he intended to facilitate a sale of MENDLESKI's leads to a Jamaican telemarketer. MENDLESKI was initially reluctant, responding that he would prefer not to sell to Jamaicans because "most of the companies are scammers." Co-Conspirator C then explained that his client could "handle jamaica!" and that it was worth the effort because "there's so much money to be made." MENDLESKI then agreed to work with

Co-Conspirator C but warned him to "be careful" because "Jamaica transactions are monitored." Co-Conspirator C responded that he had "already set up a hood ghetto team to accept payments for a small fee and i am building an encrypted chat for clients... will hook you up with that too." To this, MENDLESKI responded "cool!!!!" and then sent Co-Conspirator C a batch of leads to begin his work.

22. Before selling leads, MENDLESKI sometimes asked his clients to provide sample telemarketing scripts and signed agreements stating that they would not use the leads for illegal purposes. But if his clients refused, MENDLESKI conducted business with them anyway.

23. Frequently, MENDLESKI uploaded hard copy leads and lead lists to a Texas-based cloud computing service called FilesAnywhere. After the documents were uploaded to FilesAnywhere, MENDLESKI's clients could access them remotely from anywhere in the world.

24. On other occasions, MENDLESKI sent leads to his clients by email.

25. MENDLESKI commonly received payment from his clients via wire transfer services such as Western Union and MoneyGram.

26. The wire transfer services frequently found MENDLESKI's wire transfer records to be suspicious and thus temporarily refused to allow MENDLESKI to pick up money. Accordingly, MENDLESKI employed a network of "runners," or people who were otherwise unaffiliated with his enterprise, to collect the money on his behalf.

27. Upon receipt of the lead lists, MENDLESKI's clients defrauded the victims whose contact information they had bought from MENDLESKI.

COUNT ONE
(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

28. Paragraphs 1 through 27 of this Indictment are realleged and incorporated herein as though set forth in full.

The Conspiracy

29. From in or about January 2009 until in or about December 2014, within the Middle District of Florida and elsewhere, defendant

RONALD JOHN MENDLESKI

knowingly and willfully combined, conspired, confederated and agreed with others known and unknown to the Grand Jury, including Co-Conspirators A, B and C, to commit wire fraud, that is, to knowingly and with intent to defraud, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of material false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, for the purpose of executing such scheme and artifice in violation of Title 18, United States Code, Section 1343, all in violation of Title 18 United States Code, Section 1349.

The Purpose of the Conspiracy

30. It was the purpose of the conspiracy that MENDLESKI and others intended to enrich themselves by obtaining the personal information of tens of thousands of individuals who were inclined to listen to telemarketing pitches, and using that information to defraud those individuals through fraudulent telemarketing pitches.

Manner and Means of the Conspiracy

31. Paragraphs 13 through 27 of this Indictment are realleged and incorporated herein as though set forth in full.

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

COUNTS TWO THROUGH FOUR
(Wire Fraud – 18 U.S.C. §§ 2 and 1343)

32. Paragraphs 1 through 12 of this Indictment are realleged and incorporated herein as though set forth in full.

The Purposes of the Scheme and Artifice

33. Paragraph 30 of this Indictment is realleged and incorporated herein as a description of the purpose of the scheme and artifice.

The Scheme and Artifice

34. Paragraphs 13 through 27 of this Indictment are realleged and incorporated herein as a description of the scheme and artifice.

35. On or about the respective dates below, each such date constituting a separate count of this Indictment, within the Middle District of Florida and elsewhere, defendant

RONALD JOHN MENDLESKI

knowingly and with intent to defraud, having devised and intending to devise a scheme and artifice to defraud described above, and for obtaining money and property by means of material false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted, and aided and abetted the transmission, by means of wire communication in interstate and foreign commerce, the following writings, signs, signals, pictures and sounds, for the purpose of executing such scheme and artifice:

Count	Approximate Date	Description of Wire Communication
2	April 30, 2013	Email from Mendleski to Co-conspirator A originating from an IP address in Lee County, Florida, and containing a Microsoft Excel spreadsheet with the names and contact information of 1,200 people
3	January 10, 2014	Email from Mendleski to Co-conspirator B originating from an IP address in Lee County, Florida, and containing a Microsoft Excel spreadsheet with the names and contact information of 426 people
4	May 26, 2014	Email from Mendleski to Co-conspirator B originating from an IP address in Lee County, Florida, and containing a Microsoft Excel spreadsheet with the names and contact information of 951 people

All in violation of Title 18, United States Code, Sections 2 and 1343.

FORFEITURE

43. The allegations contained in Counts One through Four of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to the provisions of Title 18, United States Code, Sections 981(a)(1)C), 982(a)(8) and (a)(8)(A), and Title 28, United States Code, Section 2461(c).

44. Upon conviction of the violations alleged in Counts One through Four of this Indictment, the defendant, **RONALD JOHN MENDLESKI,** shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(8), any and all right, title, and interest he has in any real or personal property used or intended to be used to commit, to facilitate, or to promote the commission of such offense; and constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of the offense; and pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), all of his

interest in any property constituting or derived from proceeds obtained directly or indirectly as a result of the said violations. The property to be forfeited shall include, but not be limited to, the following:

a. A forfeiture money judgment of at least $2 million;

b. $150,000 in U.S. currency seized from the defendant's residence on November 6, 2014.

c. The real property located at 14399 Tamarac Drive, Bokeelia, Florida 33922.

45. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property under the provisions of Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c).

A TRUE BILL,

Robert J. Mastone

FOREPERSON

Date: September 28, 2016.

ANDREW WEISSMANN
Chief, Criminal Division, Fraud Section
United States Department of Justice

By: _____
TIMOTHY A. DUREE
Trial Attorney

A. LEE BENTLEY, III
United States Attorney

By: _____
JESUS M. CASAS
Assistant United States Attorney
Chief, Fort Myers Division

UNITED STATES DISTRICT COURT
Middle District of Florida
Fort Myers Division

THE UNITED STATES OF AMERICA

vs.

RONALD JOHN MENDLESKI

INDICTMENT

Violations:
18 U.S.C. § 1343
18 U.S.C. § 1349
18 U.S.C §§ 982 and 2

A ~~true~~ bill,

Foreperson

Filed in open court this 28th day
of September, 2016.

Clerk

Bail $_____