IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA	)	DOCKET NO. 3:23-CR-81-FDW
	)	
	)	**BILL OF INFORMATION**
v.	)	
	)	18 U.S.C. § 1343
HUNTER G. MELLO	)	18 U.S.C. § 1349

THE UNITED STATES ATTORNEY CHARGES:

At the specified times and at all relevant times:

Background

1. A "call center" referred to an office or workplace, often located overseas, established to manage and handle a large volume of telephone calls to or from the United States.

2. A "pop-up" was advertisement-supported software ("adware") often of a malicious nature, that temporarily locked victims' computers and displayed a message directing victims to contact a toll-free number of technical assistance for removal. Pop-ups often include inflammatory and misleading representations of diagnosing systemic network infirmities, including viruses and instances of hacking, all in an effort to delude victims into seeking costly technical assistance.

3. "Tech-support fraud" are multi-level operations that, at their core, involve material misrepresentations of viruses or other network infirmities on victims' computers. One level involves "lead generation," which is the publishing of malicious pop-ups in the furtherance of tech-support fraud. Companies that create and distribute these pop-ups are generally known as lead generators or, more commonly, "publishers," and the leads generated are actually blocks of calls spawned by pop-ups. In this sense, tech-support leads are, in reality, potential victims who dial toll-free numbers that appear on the malicious pop-ups. Once a victim makes contact with a call center, a company technician then defrauds the consumer under the auspices of providing technical assistance to resolve any number of fictitious issues identified with the victims' computer.

4. Another level of tech-support fraud involves call-routing services. These entities operate "pay-per-call" platforms that track tech-support calls from their points of origin (the victims) to the destination phone numbers (the call centers), recording the calls along the way. Publishers work with call-routing platforms to direct customer traffic to call centers based on specific types of "verticals," which is an industry term for specific types of goods and services. Publishers then work with call brokers to sell the publisher's leads to individual call centers around the world. Publishers thus sit atop the tech-support vertical, with brokers distributing blocks of pop-up-driven tech-support calls to individual call centers, which themselves rely on call traffic being re-directed by call-routing platforms. In this sense, individual call centers pay brokers acting on behalf of the publishers for quality-controlled tech-support calls, thus increasing the likelihood of the fraud succeeding.

5. Company-1, along with its affiliated entities (collectively hereinafter "Company-1"), was a company incorporated in the Seychelles that published malicious pop-ups as a means of generating customer traffic for call centers. Commonly referred to as "pops" for short, these malicious advertisements were designed by Company-1 and their co-conspirators to render customers' computers temporarily inoperable, prompting them to call toll-free numbers to be connected to individual call centers. As a publisher of pop-ups, Company-1 and its affiliated personnel worked closely with individual call centers, middle-man brokers, and call-routing platforms located around the world.

6. Individual-1 was an owner and manager of Company-1.

7. Individual-2 was also an owner and manager of Company-1.

8. Individual-3 was the owner/operator of TrackDrive, a call-routing platform that offered pay-per-call services to publishers and call centers. Individual-3 created, operated, and maintained an exclusive concierge version of TrackDrive for Individuals 1 and 2. This exclusive version was called "Moonshine." At all times relevant to this Bill of Information, Individual-3 resided in Colorado Springs, Colorado.

9. HUNTER G. MELLO was the owner/operator of ABH Media LLC, an intermediary or broker between Company-1, a "publisher" or seller of malicious pop-ups, and call centers, who purchased the malicious pop-ups to route calls to their centers. At all times relevant to this Bill of Information, MELLO resided primarily in California.

10. Individual-4 was the owner and manager of various call center companies headquartered in Charlotte, North Carolina, within the Western District of North Carolina.

11. Skype, WhatsApp, and Telegram were encrypted electronic communications platforms whose normal activities took place in interstate and foreign commerce, and had an effect on interstate and foreign commerce. These applications, which could be operated from mobile devices or desktop/laptop computers, allowed for, among other things, the sending and receiving of text messages and voice calls.

12. Corporate Entity A was an American multinational technology company with headquarters in Washington state that developed, manufactured, licensed, supported, and sold computer software, consumer electronics, personal computers, and related services.

13. Corporate Entity B was an American multinational technology company headquartered in California that designed, developed and sold consumer electronics, computer software, and online services.

The Tech-Support Scheme

14. Through Company-1, Individual-1 and Individual-2 coordinated an international conspiracy (the "Tech-Support Scheme") to defraud United States citizens by publishing malicious pop-ups that targeted United States citizens located in the Western District of North Carolina and elsewhere in the furtherance of tech-support fraud. MELLO participated in the Tech-Support Scheme by brokering the sale of the malicious pop-up "leads" to call centers. Once purchased by a particular call center, those malicious pop-ups provided phone numbers for victims to call, which directed the victims' calls to that call center. Individual-3 participated in the Tech-Support Scheme by managing the call routing platform which routed the calls from the phone number listed on the malicious pop-up to the call center which purchased the "lead." Call centers such as those owned by Individual-4 employed material misrepresentations in phone conversations with victims to trick the victims into paying for unnecessary computer software repair services.

15. Individual-1, Individual-2, and others tailored these pop-ups to particular "campaigns," which is an industry term referring to the content-specific employment of particular pop-ups over a given time. Designed with varying levels of maliciousness, some pop-ups masqueraded as "Blue Screens of Death," or BSOD for short. Other pop-ups were known as, among other things: (1) "porn pops," which flashed messages suggesting that the user's perusal of pornographic websites had resulted in the installation of harmful viruses; (2) "iOS pops," which misrepresented computer issues for Apple devices; and (3) "Desktop" or "Windows" pops, which misrepresented that Microsoft had remotely diagnosed an issue with victims' computers. Individual-1, Individual-2, and others also utilized malicious pop-ups that misrepresented technical issues related to the services, software, and devices provided and/or sold by Corporate Entity A and Corporate Entity B. Individual-1, Individual-2, and others would also configure some pop-ups to circumvent security protocols put into place by web browsers like Google Chrome. Regardless of the substance or configurations of the individual pop-ups, the end goal was the same: to delude victims into purchasing unnecessary tech-support services.

16. To proliferate pop-ups over the internet, Individuals 1 and 2 purchased thousands of domain names. Then, working with Individual-3, Individuals 1 and 2 would secure the rights to a rotating list of thousands of toll-free numbers that were embedded in the code of each pop-up. These toll-free numbers would connect to individual call centers depending on the timing, payment, and logistics of individual tech-support campaigns. Call

centers paid publishers, through third party brokers, for the malicious pop-ups to direct victims to call their call centers, so the victims could be sold unnecessary tech-support services.

17. MELLO acted as a "middleman" for Individuals 1 and 2, brokering the sale of blocks of leads to call centers and tech-support companies around the world, including to Individual-4 in the Western District of North Carolina. In coordination with Individuals 1 and 2, MELLO would sell calls at a variable rate per contact. When MELLO sold leads on behalf of Individuals 1 and 2, each call within those blocks would originate from a Company-1 pop-up. Members of the conspiracy would use Skype, WhatsApp, or Telegram to coordinate these transactions.

18. Over the course of the scheme, Company-1 became Individual-3's largest customer. To ensure that any outages on TrackDrive would not affect his business with Company-1—and in recognition of their importance as clients—Individual-3 created an exclusive version of TrackDrive that was entirely devoted to routing calls that had originated from the publishing activities of Company-1 and its related personnel. This exclusive version of TrackDrive was called "Media Moonshine, or simply "Moonshine" for short. At various points over the course of the conspiracy, MELLO acted as a payment intermediary between Company-1 and Individual-3.

19. To receive payment for their pop-ups from individual call centers, Individuals 1 and 2 used MELLO and Individual-3 as payment intermediaries. MELLO and Individual-3 would make and receive wire transfers in excess of $10,000.00 in order to distribute profits derived from victims.

Count One

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

20. Paragraphs 1 through 19 are re-alleged and incorporated by reference as if fully set forth herein.

21. From at least in or about January of 2017, through on or about August 2020, in Swain, Catawba, Mecklenburg, and Buncombe Counties (among others) in the Western District of North Carolina and elsewhere, the defendant,

HUNTER G. MELLO,

did knowingly combine, confederate, conspire and agree with others known and unknown to the United States Attorney to commit the offense of wire fraud, a violation of Title 18, United States Code, Section 1343.

Object of the Conspiracy

22. *Wire Fraud.* It was a part of and an object of the conspiracy that the defendant and others known and unknown to the United States Attorney, with the intent to defraud, having devised the above-described scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and by concealment of material facts, and for the purpose of executing and attempting to execute such scheme and artifice, knowingly transmitted and caused to be transmitted by means of wire communication in interstate commerce, writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code Section 1343.

Manner and Means

23. The defendant and his co-conspirators carried out the conspiracy through the manner and means described in Paragraphs 1 through 19 of this Bill of Information, among others.

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

NOTICE OF FORFEITURE

Notice is hereby given of 18 U.S.C. § 982 and 28 U.S.C. § 2461(c). Under Section 2461(c), criminal forfeiture is applicable to any offense for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by § 981(a)(1)(C). The following property is subject to forfeiture in accordance with §§ 982 and/or 2461(c):

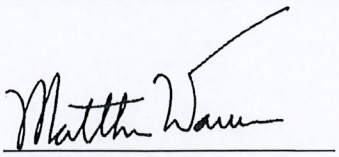
a. All property which constitutes or is derived from proceeds of the violations set forth in this Bill of Information; and

b. If, as set forth in 21 U.S.C. § 853(p), any property described in the preceding subparagraph (a) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a).

The following property is subject to forfeiture on one or more of the grounds stated above:

c. A forfeiture money judgment in the amount of at least $1,500,000, such amount constituting the proceeds of the violations set forth in this Bill of Information.

DENA J. KING
UNITED STATES ATTORNEY



MATTHEW WARREN
ASSISTANT UNITED STATES ATTORNEY

Revised AO 45 (WDNC - 3/07)

NEW CRIMINAL CASE COVER SHEET

U. S. DISTRICT COURT

(To be used for **all** new Bills of Indictments and Bills of Information)

CASE SEALED: ○ YES ◉ NO

DOCKET NUMBER: 3:23-CR-81-FDW

*If case is to be sealed, a Motion to Seal and proposed Order **must** be attached.)*

CASE NAME :US vs Hunter G. Mello

COUNTY OF OFFENSE : Mecklenburg

RELATED CASE INFORMATION :

Magistrate Judge Case Number :

Search Warrant Case Number :

Miscellaneous Case Number :

Rule 20b :

SERVICE OF PROCESS : Summons

U.S.C. CITATIONS *(Mark offense carrying greatest weight):* ○ Petty ○ Misdemeanor ◉ Felony

18 U.S.C. § 1343 and 18 U.S.C. § 1349

JUVENILE: ○ Yes ◉ No

ASSISTANT U. S. ATTORNEY : Warren, Matthew

VICTIM/WITNESS COORDINATORS: Squires, Demetra

INTERPRETER NEEDED : N/A

LIST LANGUAGE AND/OR DIALECT:

REMARKS AND SPECIAL INSTRUCTIONS: Related to case 3:21-CR-82-FDW

(Maintain form in the Attorney Work Product folder / purge before archiving)