Department of Justice

United States Attorney David L. Anderson
Northern District of California

FOR IMMEDIATE RELEASE
WWW.USDOJ.GOV/USAO/CAN
October 30, 2019

FLORIDA MAN AND CANADIAN NATIONAL PLEAD GUILTY TO HACKING/EXTORTION CONSPIRACY

Defendants admit trying to extract bounties from Uber and LinkedIn in exchange for promise to delete stolen confidential data

SAN JOSE – Brandon Charles Glover and Vasile Mereacre pleaded guilty in federal court today to their respective roles in an extortion conspiracy involving a plot to extract bounties from victim corporations in exchange for the defendants' promise to delete stolen confidential data, announced United States Attorney David L. Anderson and Federal Bureau of Investigation Special Agent in Charge John F. Bennett. The defendants admitted making extortion demands of several victim corporations including Uber and LinkedIn. The plea was accepted by the Honorable Lucy H. Koh, United States District Judge.

In pleading guilty, Glover, 26, of Winter Springs, FL, and Mereacre, 23, of Toronto, Canada, admitted that from October 2016 through January 2017, they engaged in a conspiracy to use stolen credentials to gain access to confidential corporate databases being stored on Amazon Web Services, a cloud-based storage platform After downloading confidential information from Amazon Web Services accounts belonging to the victim-corporations, Glover and Mereacre notified the victim corporations that they had found vulnerabilities in the corporations'

employees' use of the systems. The defendants then demanded money in exchange for deleting the stolen data.

"Companies like Uber are the caretakers, not the owners, of customers' personal information," said U.S. Attorney Anderson. "What gets stolen in a computer extortion belongs to your neighbors, not to yourselves. Don't be so concerned with your image or reputation. Be concerned with the real losses others have suffered. Report the intrusion promptly. Cooperate with law enforcement."

"We're dealing with the most sophisticated cyber actors in the world," said FBI Special Agent in Charge Bennett. "In order to take on those people on the front lines of the cyber security battle, we rely heavily on our valued relationships and open dialogue with private sector companies in cyber industries. Their willingness to speedily report intrusions to our investigators allows us to find and arrest those who commit data breaches.

To induce payments, the defendants used an alias and an encrypted email account to contact the victim corporations and report that their data was vulnerable. The defendants sent a sample of the stolen data to the corporations as proof their systems had been breached and then demanded payment in exchange for deletion of the data.

The plea agreements describe in some detail the defendants' communications with two companies: Uber and Lynda.com. With respect to Uber, defendants admitted they provided credentials regarding Uber's Amazon Web Services account to a "technically proficient hacker." The hacker identified archive files that contained 57 million Uber user records consisting of customer data and driver data. Defendants admitted they illegally accessed and downloaded the records from Amazon Web Services and, on November 14, 2016, contacted Uber claiming to have found a major vulnerability in Uber's computer security systems. Defendants provided a portion of the database to prove the information had been exfiltrated and then demanded payment in exchange for deleting the stolen data. The defendants' plea agreements state that on November 16, 2016, Uber agreed to pay $100,000 in bitcoin to the defendants through a third party but that, as part of the agreement, Uber demanded that the defendants also sign a confidentiality agreement. According to the plea agreements, Uber demanded that the payment for the data breach remain confidential and that the defendants destroy the data that they stole. After three weeks of negotiation, Uber made two $50,000 payments, one on December 8 and the other on December 14, 2016. Then, in January 2017, Uber informed the defendants that it had discovered Glover's true identity. On January 3, 2017, a representative from Uber met with Glover at his Florida home, where Glover admitted his role in the data breach exfiltration and signed a confidentiality agreement in his true name. On January 5, 2017, a representative from Uber met with Mereacre at a hotel restaurant in Toronto, Canada, where Mereacre admitted his role in the data breach exfiltration and signed a confidentiality agreement in his true name.

The defendants employed a similar strategy in an aborted attempt to extort funds from Lynda.com's parent company, LinkedIn. Glover and Mereacre admit that in December of 2016, they possessed information regarding over 90,000 confidential Lynda.com user accounts that the defendants had illegally accessed and downloaded from Lynda.com's Amazon Web Services account. On December 11, 2016, defendants emailed a portion of the user account information

to the security team at LinkedIn. Defendants also demanded compensation in exchange for deleting the stolen data. Rather than pay the bounty, LinkedIn sought to identify the source of the extortionist email. Specifically, LinkedIn tried to lure the writer of the email to enroll with a third party to assist in the negotiation of terms for payment to the defendants. In this way, LinkedIn hoped to identify the extortionist and notify law enforcement of the plot. Defendants told LinkedIn's representatives, "[p]lease keep in mind, we expect a big payment as this was hard work for us, we already helped a big corp which paid close to 7 digits, all went well." The defendants stopped communicating with LinkedIn in January 2017, and the company did not pay defendants for the data or for confidentiality.

Glover and Mereacre both were charged by a Superseding Information on October 30, 2019. Each defendant was charged with one count of conspiracy to commit extortion involving computers, in violation of 18 U.S.C. §§ 1030(a)(7)(B) and (c)(3)(A). Today, Glover and Mereacre pleaded guilty to their respective roles in the conspiracy.

The defendants have been released on bond pending sentencing. Judge Koh has scheduled a status conference regarding sentencing for March 18, 2020. The maximum statutory penalty for conspiracy to commit extortion involving computers is five years imprisonment and a fine of $250,000. The court may also order an additional term of supervised release and restitution; however, any sentence will be imposed by the court only after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

Assistant U.S. Attorneys Susan Knight and Amie Rooney are prosecuting the case with the assistance of Elise Etter and Lakisha Holliman. The prosecution is being handled by the Office of the U.S. Attorney, Northern District of California's new Corporate Fraud Strike Force and is the result of an investigation by the FBI.

Further Information:

Case #: 18-cr-00348 LHK

A copy of this press release will be placed on the U.S. Attorney's Office's website at www.usdoj.gov/usao/can.

Electronic court filings and further procedural and docket information are available at https://ecf.cand.uscourts.gov/cgi-bin/login.pl.

Judges' calendars with schedules for upcoming court hearings can be viewed on the court's website at www.cand.uscourts.gov.

All press inquiries to the U.S. Attorney's Office should be directed to Abraham Simmons at (415) 436-7264 or by e-mail at Abraham.Simmons@usdoj.gov.