OFFICE of PRIVATE SECTOR
LIAISON INFORMATION REPORT (LIR)

INFORMATION TECHNOLOGY SECTOR

6 June 2019 **LIR 190606001**

Criminals Misrepresenting Companies' Technology Support Departments to Fraudulently Obtain Personal and Financial Information

The FBI's New York Office, in coordination with the FBI's Office of Private Sector, is providing this information to private sector partners regarding criminals posing as technology support representatives to obtain personal and financial information. The perpetrators gain trust from victims by impersonating a representative from a legitimate or an illegitimate technology company. They mislead the victims by offering computer services to resolve a range of computer security and operations issues. When victims subscribe to the fraudulent services, the perpetrators gain access to their personal identifiable information and financial accounts. Some examples of this scam include:

- In October 2018, a victim received a phone call from a perpetrator who claimed he needed remote access to repair the victim's computer issues. The perpetrator told the victim to send funds to the perpetrator's account numbers because the victim was overpaid for a refund. As a result, the victim incurred a loss of approximately $416,000.

- In or around April 2018, a victim's computer displayed a message after it froze instructing the victim to call a specific phone number to correct a computer "problem". The victim called and allowed the individual on the telephone remote access into his computer. The victim thought the individual fixed the computer issue and sent a check for approximately $1,400 to the tech support company for the service. The victim researched the company, realized it was a scam, and stopped payment on the check.

- In December 2017, a perpetrator posing as a representative of a computer service company that a victim used to maintain the operating system on the victim's computer, told the victim he or she would receive a refund. The perpetrator used a computer program to connect to the victim's machine to transfer money between the victim's accounts, stealing approximately $118,700.

According to FBI information, criminals will likely increase their use of technology support scams due to the ease of misleading victims by posing as technology support representatives and the prospect of financial gain. Criminals may also expand their activities to target start-up companies and small businesses who do not have a permanent or sufficient technology support staff.

Indications of criminals conducting technology support scams include, but are not limited to the following:

- Complaints from customers reporting they were defrauded by an individual posing as a technology support representative
- Complaints from customers reporting pop-up messages directing the customer to call a specific

phone number for IT services

- Complaints from customers who sent wire transfers to countries such as Hong Kong and Malaysia to pay for IT services
- Complaints from customers who paid for IT services via prepaid cards or money transfer applications
- Complaints from customers who received an unsolicited phone number for an IT company who appeared legitimate
- Complaints from customers who provided their bank or credit card information to receive a “refund”

If you or your company are victims or become aware of a technology support scam, report it to your security/fraud department, the FBI’s Internet Crime Complaint Center at www.ic3.gov, local FBI Field Office, and/or the Federal Trade Commission at https://www.ftc.gov/complaint. Routinely train personnel on indicators of technology support scams and reporting procedures.

This LIR was disseminated from OPS’s Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices