IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	**SUPERSEDING INDICTMENT**
	)	
Plaintiff,	)	**FILED UNDER SEAL**
	)	
v.	)	JUDGE DONALD C. NUGENT
	)	
ROMEO VASILE CHITA,	)	CASE NO. 1:10CR392
a/k/a "Rich,"	)	
TEODOR VIOREL RADU,	)	18 U.S.C. § 1962(d)
DANIEL MIHAI RADU,	)	18 U.S.C. § 1349
IONUT CHERA,	)	18 U.S.C. § 1956(h)
a/k/a "Ciceo,"	)	18 U.S.C. § 371
CLAUDIU VIRGIL TURLEA	)	18 U.S.C. § 1963 (forfeiture)
a/k/a "Biggie,"	)	18 U.S.C. § 981 (forfeiture)
a/k/a "Bigs,"	)	18 U.S.C. § 982 (forfeiture)
a/k/a "Bighi,"	)	
MANUEL TUDOR,	)	
a/k/a "Manu"	)	
a/k/a "Man,"	)	
a/k/a "Marius,"	)	
CAROL JURJA,	)	
a/k/a "Crapu"	)	
DANIEL UNGUREANU,	)	
a/k/a "Frank,"	)	
a/k/a "Dan,"	)	
DUMITRU NICOLAITA,	)	
a/k/a "TB,"	)	
	)	
Defendants.	)	

COUNT ONE
(Racketeering Conspiracy)

The Grand Jury charges:

General Allegations and Definitions

At all times relevant to this indictment, unless otherwise alleged:

1. The Internet is a global network connecting millions of computers and computer networks to each other allowing them to communicate and transfer information. Using, among other things, a system of wires, cables, routers, and circuits, the Internet allows the communication and transfer of information in interstate and foreign commerce. One type of information transferred across the Internet is email, which is an electronic communication or message sent across the Internet. Another type of information involves online banking and information transferred in connection to accessing bank accounts and transferring money over the Internet.

2. "Phishing" is an attempt to fraudulently acquire personal information by sending an email which falsely claims to be from an established legitimate entity. One type of phish email directs the user to open an attachment to the email. Opening the attachment usually results in the installation of malware without the user's knowledge. The malware is often in the form of a keylogger. The keylogger captures sensitive and confidential information entered on the computer by the victim during the course of the victim's business and financial activities.

3. "Spear-phishing" is a term used to describe highly targeted phishing attacks. Spear-phishers send emails that tend to be much more focused and detailed than a typical phish. Spear-phishers also target their victims more carefully than typical phishers or spammers. An

example of "spear-phishing" is sending an email to an individual believed to access on-line banking services using secret passwords for the purpose of stealing that information.

4. "Keylogger" means a computer program or programs that surreptitiously capture the keys typed on a computer and forwards that information to the individuals who caused it to be installed or to a place designated by them. Through this technique, individuals are able to secretly obtain the user identification and passwords for bank accounts as soon as the user of the infected computer logs into their account on-line. After obtaining this information, the individuals execute unauthorized ACH and wire transfers to accounts that they control.

5. "Mule" or "money mule" is an individual recruited to receive and transmit unauthorized electronic funds transfers from deposit accounts to designated individuals in the United States or overseas. Depending on the scheme, a mule is solicited by individuals who (1) have gained unauthorized access to the online deposit account of a business or consumer or (2) have otherwise fraudulently obtained money or funds. In many instances, the mule is located in the United States and opens and controls a deposit account that is intended to accept the unauthorized transfer from a victim's account. Often in these instances, the money mule is then instructed to quickly withdraw the funds and wire them overseas after deducting a commission. In some cases, a money mule may be instructed not to open bank accounts but instead to pick up or send funds using a money transfer service such as Western Union or MoneyGram.

6. "Spam" generally is an email message that is sent in bulk to recipients without prior request or approval. The origin of the spam is almost always masked or falsified to prevent any identification of the sender.

7. "Malware" is an abbreviated term for "malicious software." Malware refers to