Attachment A

Common tactics used to steal identity and login credentials

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the investor protection checklist are intended to help you and your family better protect yourselves against such activity.

• **Malware.** Using malicious software (hence, the prefix "mal" in malware), criminals gain access to private computer systems (e.g., home computer) and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.
How it works: While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email.

• **Phishing.** In this ruse, the criminals attempt to acquire sensitive personal information via email. Phishing is one of the most common tactics observed in the financial services industry.
How it works: Masquerading as an entity with which the victim already has a financial relationship (e.g., a bank, credit card company, brokerage company, or other financial services firm), the criminals solicit sensitive personal data from unwitting recipients.

• **Social engineering.** Via social media and other electronic media, criminals gain the trust of victims over time, manipulating them into divulging confidential information.
How it works: Typically, these scammers leverage something they know about the person – like their address or phone number – to gain their confidence and get them to provide more personal information, which can be used to assist the criminal in committing fraud. Social engineering has increased dramatically, and many times fraudsters are contacting investors by telephone.