Fraud Concepts and Definitions

- **Malware**

Malware (malicious software) is a broad collection of software that is installed onto a computer without the knowledge of the computer owner or user with the intent of performing some malicious task. Malware includes Banking Trojans (see below), spyware, dishonest adware and viruses.

- **Computer Virus**

Viruses are a specific type of malware that can automatically replicate themselves, spreading to other computers. They can be used for a broad range of malicious activity.

- **Banking Trojan**

Trojans are a particular type of malware, named after the Trojan horse. Banking Trojans are used in real time by fraudsters who wait until the account holder logs in and then they manipulate the online banking session in the background without the user knowing it.

- **Man-In-the-Browesr (MITB) / Man-In-the-Middle (MITM)**

Man-In-the-Browser malware is a specific type of Banking Trojan that enables a fraudster to transparently take over control of an online banking session or change the details of an online banking session without the knowledge of the victim.

- **Other Types of Malware**
- Key Logging malware waits for the user to login to their online banking provider and then keeps track of all keystrokes entered, which would include user name, password, answers to challenge questions, and PINs.
  - Spyware is a category of malware that is designed to collect small pieces of information about users without their knowledge. Key logging malware is one type of spyware.
  - Internet bots, also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet. Malicious use of bots includes the coordination and operation of an automated attack on networked computers, such as a DDoS attack.

- **Phishing**

Email from what appears to be a known, trusted organization, such as a bank, credit card company, large corporation, industry association, or government entity. The email typically describes some urgent situation that requires the victim to confirm personal or financial information. When the victim clicks on the link in the email they are directed to a fake site that captures sensitive information or it downloads malware onto their computer.

Variations on Phishing: All have the same objective of getting the victim to divulge online banking credentials or other personal information:

- Vishing: voicemail or live phone calls
- Smishing: text messages sent to smart phones
- Twishing: Tweets with links to spoofed websites

- **Social Engineering Attacks**

This is the same as phishing. Social Engineering involves manipulating people into performing actions or divulging confidential information, typically through a live phone conversation. This often relies on the fraudster knowing something about the victim in order to establish credibility, after which they can then get the victim to divulge additional information.