Types of Fraud Attacks

- **Clean Fraud:**
    - The term describes the willingness and ability of thieves to provide more and better personal information in card-not-present transactions, information that in isolation gives the appearance of legitimacy to the transaction.

- **Account Takeover:**
    - Account takeover is one of the more prevalent forms of identity theft. It is becoming increasingly prominent and is a growing point of financial exposure for businesses and consumers. The takeover occurs when a fraudster obtains an individual's personal information such as an account number, password, username, or Social Security number and changes the official contact information (mail/e-mail address) or adds another user to an existing account. By doing this, the fraudster establishes an opportunity to make transactions without the victim's knowledge.

- **Friendly Fraud:**
    - Also known as "friendly fraud chargeback," this fraud occurs when consumers make an Internet purchase with their own credit card and then issues a chargeback through the card provider after receiving the goods or services. When a chargeback occurs, the merchant will always be responsible for loss of funds, regardless of what it did to verify the transaction. There is no way to verify the authenticity of the transaction, which is in fact legitimate, because the consumer is the one who is not legitimate.

- **Identity Theft:**
    - Identity theft is a when someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name.

- **Phishing:**
    - Phishing (also called pharming or whaling) e-mails trick people into sending money or providing personal information such as usernames, passwords, credit card details, and Social Security numbers to unauthorized individuals who hijack their information and use it to commit identity theft.

- **Affiliate Fraud:**
    - In this type of fraud, bogus activity generated by an affiliate attempts to generate illegitimate, unearned revenue. Fraudulent activity by affiliates comes in both automated and non-automated varieties. Automated scripts attempt to mimic the activity of legitimate, human visitors. Non-automated schemes may involve coordinated efforts by humans actively generating excess clicks or registrations.

Types of Fraud Attacks

- **Re-shipping:**
    - In re-shipping, or postal forwarding, scam victims typically are offered an at-home job that involves re-packaging stolen goods--frequently consumer electronics--and forwarding them, often outside the U.S. Scammers ask victims to pay their own shipping charges, and pay reimbursement and compensation with a fake check. In addition to seeing their own paychecks bounce, those who fall for re-shipping scams may be liable for shipping charges and even the cost of goods purchased online with stolen credit cards.

- **Botnets:**
    - A botnet is a collection of compromised computers under the remote command and control of a criminal "botherder." Most owners of the compromised computers are unwitting victims. They have unintentionally allowed unauthorized access and use of their computers as a vehicle to facilitate other crimes, such as identity theft, denial of service attacks, phishing, click fraud, and the mass distribution of spam and spyware. Because of their widely distributed capabilities, botnets are a growing threat to national security, the national information infrastructure, and the economy.

- **Triangulation Schemes:**
    - Triangulation is another method of credit card fraud. The fraudsters operate from a web site and offers goods at heavily discounted rates and with shipping before payment. The fraudulent web site appears to be a legitimate auction or traditional sales web site. The customer must provide information, including name, address, and valid credit card details to the web site. Once the fraudsters receive the details, they order the goods from a legitimate web site using another stolen credit card number and apply for the goods with the customer's name and address. The fraudsters then purchase other goods with customer's credit card numbers. This process causes initial confusion for authorities so the fraudulent Internet company can operate long enough to accumulate a vast amount of goods purchased with stolen credit card numbers.

Sources: (2012, November 26) Scam alerts. Internet Crime Complaint Center (IC3). (2013, January, Volume 21, Number 1) Magloclen Network, Analytical Articles, Jessica Rodriguez.