ANALYSIS

On the Essence, Types and Indicators of Mass Marketing Fraud Schemes

In order to raise awareness among financial and non-financial institutions operating in the Republic of Armenia, as well as among the general public, an analysis has been conducted, based on the local and international experience with the aim of describing the nature of mass-marketing fraud schemes (hereinafter MMF), the essence of its phenomenon, the types, as well as the detection of the application of such schemes.

1. The Essence of MMFs

Mass-marketing fraud (MMF) is a scheme that utilizes modern mass communication including telephone, internet, electronic mail, television, radio and sometimes personal contacts to identify, contact, solicit, and fraudulently obtain money, funds, or something of value by convincing or requesting multiple victims in one or more jurisdictions.

MMF was first identified in a handful of countries a few decades ago. Now, it is a global problem, suggesting the need for government officials to work multilaterally to combat this criminal activity. MMF scams are usually perpetrated through mass communication means abroad, usually by a criminal organization. Fraud proceeds are remitted in different directions to conceal the source. Criminal organizations recruit "employees" and place them in countries around the world to perpetrate schemes and move the illicit proceeds.

The methods perpetrated by fraudsters include the targeting of victims in numerous countries on multiple continents, using the advantage of international borders to hinder legislative authorities prohibiting the schemes. The schemes can be perpetrated from anywhere in the world, making their identification difficult and time consuming.

The guilt, shame, and embarrassment of these crimes felt by victims often take a psychological toll. The impact on victims of MMF includes the loss of personal savings or property, physical risks or threats of violence, depression or health issues, and even contemplated, attempted, or actual suicide.

2. *MMF Types*

MMF encompasses a wide range of schemes, which are designed to separate individuals and businesses from their property, money, services, or information. The following types of MMF schemes are the most frequently reported worldwide:

1) **Advance-Fee Fraud Schemes** use solicitations that entice victims with improbable promises of enormous wealth in exchange for up-front payments of fictitious taxes and fees.

Example: Person A receives an e-mail with the following contents: "I am the son of the former president of Country B. My father died leaving me a great fortune, but the current Government froze a part of those funds and made me a political refugee. In these circumstances it is not advisable to hold the money in the name of a member of our family. I would prefer to

temporarily transfer the money to your account, if that is possible. You will receive 5% of the funds in exchange. Please respond if you are interested in this offer".

Further communication with the "owner" of huge funds reveals that for certain "substantiated" reasons, he does not have money to pay for the bank transfers or for the preparation of the needed documents; therefore, he asks Person A for an advance payment on the condition of paying it back later on. Once the fraudster succeeds in abusing confidence and squeezing certain amounts of money from Person A, he ceases communication via e-mail.

Moreover, in some cases the account number and personal data of Person A may be abused to embezzle money from his/her card or to use it as transit account in various money laundering schemes.

2) **On-Line Auction Fraud Schemes** defraud unwitting buyers and sellers and exploit the anonymity of the Internet to conceal the perpetrators' locations and identities. Criminal techniques include wire transfer and overpayment schemes, late and non-deliveries, and misrepresentation of a product's true condition.

Example: Person A, who looks for a rare ancient coin, comes to know that a little known online auction website has such coin for sale at a low opening price. He/she manages to become the "successful" bidder and to buy the coin at a price lower than expected, being informed that half of the price should be paid right away while the other half may be paid upon delivery. After transferring the requested funds, Person A never receives the coin he/she "bought". Moreover, the transfers within such schemes are made either through a money remittance systems or through on-line payment systems, or through an intermediary in the country of Person A, by all means avoiding a direct bank transfer which would enable detection of the fraudster's identification data, country and bank account number.[1]

3) **Charity Fraud Schemes** solicit financial contributions, but use little or none of the donations to support the charities or causes for which the funds were ostensibly raised for. Perpetrators exploit sympathetic causes, legitimate charities' names, and refer to the need to withstand humanitarian or environmental disasters.

Example: Charity Foundation B, which was established in Country A to help people who suffered from a disastrous hurricane, legitimately collects funds from individuals and companies. Person C, who has nothing to do with Charity Foundation B, introduces himself/herself as its authorized individual and sends e-mails to a number of people asking on behalf of the foundation to transfer sums to an account supposedly opened to collect donations for helping the victims of the hurricane, but one that is factually controlled by the fraudster. The sums collected on this account are then used at the discretion of Person C, naturally not for helping those who suffered from the hurricane.

4) **Counterfeit Check Fraud Schemes** require that the recipient deposits a check or money order into his/her bank account, and then wire transfers a portion of the value of the check

[1] For example by Moneygram, Sigue Money Transfer and etc.

or money order back to the sender/perpetrator of the scheme. It is often the case that, weeks after the victim deposits the check or money order, the bank informs the victim that the financial instrument was counterfeit and holds the victim liable for the face value of the instrument.

Example: Company A sells high value goods. Customer B offers to pay for the goods by check referring to the large amount of the transaction. Company A agrees to accept the payment by check and to supply the respective goods. Company A accepts the payment in check and supplies the respective goods. However, as soon as the check is deposited with the bank for encashment, they find out that it is forged.

Moreover, in the scheme described above Customer B may either be the one who produced the forged check or the intermediary who personally or by mail, organized the encashment of forged checks against a commission/ payment.

5) **Emergency Assistance Fraud Schemes** require immediate financial assistance for bail or emergency medical expenses. The perpetrator poses as a person whose family member or close friend (often a college student studying abroad) needs financial help to be released from detention or to get urgent medical assistance.

Example: Person A spends some time in social networks and, based on certain common interests, gets acquainted with Person B. After a period of communication Person B informs Person A that his wife has had an accident and needs an urgent surgery. In view of the urgency of the payment for the surgery on one hand and the difficult financial situation on the other hand, Person B asks to make a wire transfer to a certain account (on the condition of returning the funds later on). In addition, such schemes may utilize both mass mailing techniques and more targeted approaches by finding out beforehand personal identification data, family membership and status of the potential victims in social networks.

6) **Employment and Business Opportunity Fraud Schemes in which the organizers** promise easy money in exchange for minimal effort and little or no experience. These include pyramid scams, work-at-home, mystery shopping and mail reshipping schemes, attractive offers for employment abroad etc. The schemes frequently require job applicants to make costly, up-front purchases of supplies and educational materials, and may employ counterfeit financial instruments to engage victim participation.

Example: A website specializing in the sales of exclusive watches, which are not available at retail sale and other public service networks, explores a promotional program enabling customers, who have purchased a certain batch of products, to become agents and earn money by recruiting new customers. However, later on it becomes clear that the products are significantly over-priced, and that the batch of the products that is needed to be purchased for becoming an agent is too large for being resold within a reasonable timeframe.

7) **Foreign Lottery and Sweepstakes Fraud Schemes** promise nonexistent monetary awards in exchange for the advance payment of fictitious fees and taxes.

Example: While Person A surfs a website, a pop-up message notifies that he/she is the 100.000th visitor of the website and has been awarded a large prize on that occasion. To collect the award, Person A is offered to call a specific phone number, and when he/she makes the call he/she finds out that the income tax has to be paid before getting the award. Naturally, payment of the "income tax" does not result in receiving the award (insofar as the fraudsters stop answering phone calls, put forward new requirements and etc.).

8) **Investment Fraud Schemes** promise high yields on securities, real estate; stakes in oil drilling ventures, coins, gems, and other commodities. This is also known as "boiler room" fraud. Such schemes include penny stock schemes and high-yield investment programs.

Example: Person B who is resident to Country A, receives a call from Person C introducing himself/herself as an authorized individual of the "well-known" Company E listed in the stock exchange of the Country D, offering to buy stocks in Company E at 30% discount. Person C describes the far-reaching prospects of the company and promises 100% net profit on the invested amount to be gained both through the increase in the market price of the stocks and through dividends to be paid. He/she advises that the decision should be made within a few hours since issued stocks are sold out very quickly.

Person B checks the information available in the Internet on Company E (usually restricted to information published by Company E itself) and, considering the offer to be attractive enough, decides to invest 7.000 US dollars. One month later Person B gains significant dividends and finds out that market price of the stocks has increased by 30%.

Soon he/she receives another call from Person C telling him/her that one of the shareholders of the company is selling his/her stocks at extremely beneficial terms and that he/she can make an investment of 100.000 US dollars and that the decision should be made within a few minutes.

Sometime after making the investment Person B finds out that the stocks of Company E have depreciated, and since it is registered in Country D, there are no meaningful steps that he/she as the resident of Country A could take to get back his/her investment.

9) **Loan, Credit Card, and Grant Fraud Schemes** are fraudulent offers of loans, credit cards, and grant schemes in exchange for advance payments of administrative and finder's fees. Perpetrators usually target individuals and small businesses.

Example: Person A receives an e-mail from Person B, who introduces himself/herself as an authorized individual from the authoritative International Organization C, notifying him/her that he/she has been selected as the beneficiary of an annual grant. Person A is requested to send his/her identification data to receive the grant, which has to be spent for educational, business or social purposes. Person A fills in the submitted form his/her identification data and sends it to Person B. With the next e-mail, Person B advises that a 1 million US dollar check has been issued on his/her name and will be delivered upon the payment of postal delivery fees (50 US dollars) and insurance charges (400 US dollars). Persons A makes these payments, as well as additional

payments requested for various reasons thereafter, but never happens to receive the desired "grant".

10) **Mass-Marketing Fraud Schemes Targeting Businesses** are fraudulent invoice scams and deceptive solicitations intended for the purchase of discounted supplies, or advertisements in nonexistent business directories or poorly-crafted websites.

Example: Company A using services of Business Directory B receives an e-mail as if from the latter, but in reality from the perpetrators of the fraudulent scheme, requesting an urgent payment for further maintenance of the contacts and advertisement of Company A in its information resources. The attached invoice not only claims an amount larger than usually collected for the services, but also specifies a different account number, which is factually controlled by the fraudsters. The staff member of Company A, who fails to examine the e-mail diligently and gets his doubts dispelled through additional communication with the "representatives" of Business Directory B, makes the requested payment.

11) **Product Misrepresentation Fraud Schemes** are deceptive offers of goods and services, including credit protection and repair programs, vacations, timeshares, green card application services, and health care treatments. While these schemes vary widely in their nature, scope, and implementation, victims commonly fail to receive the purchased products or services, or receive worthless or significantly less valuable products or services than those promised.

Example: Person A receives an e-mail advertising a medicine, which enables the user a reduction of weight by 15 kg in only 3 weeks. He/she makes the payment to Reseller B and gets the medicine, which not only fails to provide the promised outcome but also causes unrecoverable damage to his/her health. Later on, it becomes known that the medicine had not been licensed by the public healthcare authority of Country C because of its side effects.

12) **Recovery Fraud Schemes** target prior scam victims with fraudulent offers to facilitate the return of the victims' funds following the advance payment of certain administrative and other fees. Perpetrators of recovery schemes often pose as lawyers, law enforcement officials, or other government officials.

Example: Person A, who fell victim to one of the various fraud schemes, receives an e-mail from Person B introducing himself/herself as an employee of the Police of Country C (from where the perpetrator of fraud acted). He/she claims to be the investigator in charge of the case for recovering the loss incurred by Person A and asks for a certain amount to cover the expenses of investigation. It is also possible that, during the negotiations, Person A is requested to submit his/her account details in order to receive compensation. However, in reality, Person B is one of the perpetrators of the previous fraud, whereas the promises to recover Person A's losses as well as the requests to submit account details are solely meant to fraudulently squeeze more money from him/she.

13) **Romance Fraud Schemes** target users of Internet dating and social networking sites by feigning romantic interest, securing victims' trust and affection through regular intimate conversations and exchanges of small-value gifts, and then exploiting the relationship to fraudulently obtain money and valuable merchandise. Romance scam victims have reported sending money to facilitate the purchase of travel documents and airline tickets, pay for medication and hospital bills, fund charitable works programs, and help perpetrators recover from personal financial difficulties.

Example: Person B gets acquainted with Person A on a social networking website. Due to regular and long-lasting communication, Person A manages to secure trust and affection of Person B. They build plans for future relationships, cohabitation and possibly some joint business activities. Thereafter, Person B regularly asks for various reasons and receives financial help from Person A. When the money sent by Person A grow to constitute a significant amount, or whenever Person A demonstrates suspicions about the real purposes of the communication, Person B stops the communication.

14) **Traditional West African Fraud Schemes** entice victims with promises of immediate and enormous wealth. Perpetrators claim to need a victim's financial assistance to transfer or embezzle money, often millions of dollars, from a foreign country or company in exchange for a portion of the transferred or embezzled funds. Traditional West African fraud schemes are often termed "419 frauds," after the section of the Nigerian criminal code pertaining to fraud. Common West African Fraud solicitations include the following:

14.1) **Black-Money Fraud Schemes** solicit victims to purchase special cleansers to remove dye from paper currency that has, for various reasons, been blackened and rendered unusable (or, alternatively, to transform pieces of ordinary black paper into real dollar banknotes).

Example: Person A sends an e-mail to thousands of users stating that he/she somehow managed to import into Country B, banknotes worth 1 million US dollars, which had been blackened to conceal their being legitimate paper currency. He/she advises that there is a liquid enabling safe removal of the black dye and recovery of the original color and shape of the banknotes. He/she agrees to submit the liquid free of charge on the condition that he/she gets 30% of the face value of the recovered banknotes. User C decides to check this and orders blackened banknotes for 1.000 US dollars, and the cleanser. The experiment proves to be successful, and the perspectives of earning easy money make User C order blackened banknotes for 100.000 US dollars against an up-front payment of 30.000 US dollars. However, this time he/she reveals to have received pieces of black paper only.

14.2) **Inheritance Fraud Schemes** involve perpetrators requiring victims that pay fictitious fees and taxes to claim nonexistent estates of previously-unknown and now-deceased relatives.

Example: Person A receives an e-mail from Person B notifying that he/she is the personal lawyer of a wealthy Person C, who passed away months ago. Person B advises that Person C left a huge fortune and has no heirs, therefore, the state would inherit that tremendous wealth. Person

B assumes to take care of the legal processes, against a fee, in a way that Person A is recognized as the only heir of Person C to inherit his/her huge fortune. In further communication, Person B requests Person A to send certain amounts for legal implementation, tax expenses and other reasons, and embezzles them.

15) **Contractual Offer Fraud Schemes with Significant Terms Veiled** involve perpetrators obtaining data on potential victims and approaching them through the Internet or postal delivery to send various contracts, with the most important terms of those contracts articulated in a manner unnoticeable at first glance, e.g. in very small font size, at the very end of the contract or in the footnotes section. The purpose of the scheme is that the victims interested by the apparently beneficial conditions of the offer sign and send back the contract without detailed consideration, thus making them obliged to make the relevant payments as per the contract.

Example: Person A receives a contract through postal delivery, whereby Person B proposes him to act as the person in charge of a to-be-organized trade event, e.g. an exhibition (previously Person B had done some similar work, and Person A had access to that information). Person A is simply requested to check accuracy of his/her personal data, sign the contract and send it back to the organizers.

Furthermore, while there is a clearly visible statement at the beginning of the contract that the nomination of Person A for the said position is entirely free of charge, within the body text of the contract there is a provision articulated in an unnoticeable place and manner that the person in charge of the to-be-organized exhibition shall be obliged to pay Person B for solicitation an annual fee equaling 1.000 US dollars for three consecutive years, even in case if the event is postponed or cancelled.

Person A signs and sends back the contract, which, at the first glance, does not result in any obligations for him/her. Later on, however, he/she receives a payment claim from Person B in accordance with the provisions of the contract. Victims of such fraud schemes often make the requested payment feeling themselves in a legal stalemate.

16) **Call from Competent Bodies Fraud Schemes** explore call centers established by perpetrators to make massive calls to users in different countries and to introduce themselves as representatives of competent bodies. They notify the potential victims that, inadvertently, they have become part of money laundering or other criminal offenses and have to transfer a certain amount to the specified account in order to escape responsibility.

Example: Person A receives a call from Person B (who has already collected some information on Person A) from Country C, who introduces himself/herself as a staff member of an international structure to combat money laundering and terrorist financing. Person B advises and assures Person A that he/she has inadvertently become part of transactions related to illegal drug trafficking, and that in order to withdraw the criminal proceedings, Person A would need to transfer a certain amount to a specified account. Perpetrators often select victims from among those who, for some reasons, would not opt to apply to law enforcement authorities.

17) **Hacker Intervention into Business Relationships Fraud Schemes** involve hackers having obtained access to the correspondence between business counterparties, when they start intervening the communication between them by means of sending letters on behalf of a counterparty to the other. The aim of this is to embezzle funds by redirecting payments made in the course of regular business relationships to the accounts controlled by perpetrators.

Example: Company A communicates via e-mail with its foreign counterparty, Company B, to make a regular order for a batch of products amounting to 30.000 US dollars. Starting from a certain point, Person C manages to intervene in the communication in a stealthy manner that goes unnoticed by both Company A and Company B so that the exchanges of e-mails between the companies begin to go through him/her. Thereafter, Person C continues communication with Company A on behalf of Company B and, immediately before the payment is to be made, notifies about the change of their account number and asks to make the payment to the new account specified by him/her. Company A, who has no suspicions about the fraud and, therefore, does not even attempt to contact Company B through alternative means of communication, makes the payment, which Person C withdraws immediately and closes the account.

18) **"Selling" of Goods at Obviously Lower than Market Prices Fraud Schemes**, in which criminals make announcements regarding the sale of products (cellular phones, cars, apartments, etc.) at affordable prices on various websites, while the potential victims who seek to buy those goods are required to ensure the availability of their funds by making an informal money transfer and sending the transfer of documents to them, without mentioning the unique reference number of the transfer. After receiving the information concerning the transfer, the perpetrators, by using the unique reference number, are able to, in some devious way, receive some of the transferred funds in another country.

For example: Person A, while visiting an Armenian sales website, finds a post regarding the sale of an automobile with a price that is significantly lower than the market price, and in the post he/she finds a contact number that is an international number. After getting into contact with Person B, Person A is notified that Person B used to live in Armenia for a while, where he/she owns a car, which he/she wants to sell. Additionally, Person B states that he/she is coming to Armenia for a few days and wants to quickly formulize the sale of the automobile and the transaction. After agreeing the terms of the sale, Person B notes that in order that he/she no longer holds talks with other potential buyers, he/she needs to be convinced that Person A has the required funds to purchase the automobile. With that reason, Person B asks Person A, with the use of fast money transfers systems, to make a "test" payment from a trustworthy individuals' account and to send a picture of the payment document electronically but by covering unique reference number by the use of his/her hand.[2] Person B also assures Person A that Person A can cancel the transfer and receive the money back.

Moreover, Person A makes the money transfer to Person B by using the name and account of one of his/her close Acquaintance C, by taking a picture of the transaction and sending it to

[2] For example: Moneygram, Sigue Money Transfer and etc.

Person B. After receiving the picture and information, Person B, who has a sample copy of an Armenian passport and on that basis makes a fake passport by the name of Acquaintance C, which he/she makes in a commonly known way (for example by hacking) and discovers the unique transfer reference number, and from a third country receives the the amount with the use of a false passport.

Some of these MMF schemes are inter-related with the others. For example, lottery fraud schemes sometimes use elements of counterfeit check fraud schemes to perpetrate the scam; pyramid and Ponzi schemes are also defined as investment schemes; and romance schemes can also involve advance fee frauds, etc.

Identity theft is often used to perpetrate MMF schemes, particularly on the Internet. It exploits information such as an individual's name, credit card number, bank account number, or other personally identifying data. Once the information is stolen, it is used without the victim's knowledge in cyber locations the victim may be unfamiliar with (e.g. websites, blogs, email, etc.)

MMF schemes are committed by coordinated actions of fraudsters and the illicit proceeds are received by their counterparts in different countries or even on different continents in the world. For example, a fraudster sitting in a café in Africa may use the Internet to perpetrate an emergency assistance scheme to defraud a U.S. citizen, instructing the victim to send his/her money to a fraudster in Asia, who would withdraw his/her portion of criminal proceeds and forward the funds to the fraudster 'in charge' in Europe. Fraud networks are designed to perpetrate the activity as quickly and easily as possible.

3. MMFIndicators

The following MMF indicators can enhance the ability of the financial industry to recognize MMF proceeds when they are encountered:

- Repetitive and rapid in-and-out transactions,
- Large cash deposits and wire transfers,
- Third party transfers from overseas followed by immediate (large) cash withdrawals,
- Cash deposits by third parties,
- Use of cash couriers,[3]
- Multiple structured and interrelated transactions,
- Round sum transactions,
- Non face-to-face transactions (including those through the use of money machines),
- Wire transfers between entities with no relationship or connection,
- Transfers to or from high risk money laundering jurisdictions without an apparent business purpose,
- Use of false documentation when transferring funds,
- Use of forged checks when carrying out transactions,

[3] I.e. persons who carry out physical transportation of cash across the customs boundaries of nations

- Vulnerable individuals (e.g. elderly) sending money overseas without purpose and using money service businesses,
- Individuals behaving defensively when questioned about money transfers,
- Large amount transactions inconsistent with client profile,
- Use of personal account for business transactions,
- Use of multiple money service businesses in the same geographical location,
- Credit card Internet transactions,
- Use of Internet-based payment systems,
- Multiple transfers transacted on the same day and to the same beneficiary,
- Large number of bank accounts by a customer at the same financial institution.

Identification of one or several indicators as articulated above is not strictly defined as an established fact of having detected a victim or a perpetrator. A victim may be unable to send money to a fraudster due to lack of funds. The fraudster will in turn tell the victim to move money for them in exchange for payments. Therefore the victim will become a perpetrator of the criminal network. The persuasion or threat of violence enables the fraudster to convince the victim they are helpless or vulnerable if they do not comply. This creates a cycle of criminal activity that is difficult to break.

Fund transfers are accomplished through various types of transactions. The money can be deposited and withdrawn from one or many bank accounts, either in cash or through wire transfers where the account holders use false documentation; moving cash through money service businesses where an account is not necessary as a means of hiding transactions; transferring money to foreign jurisdictions quickly to evade suspicion and/or reporting requirements; and using identity theft to open accounts or transfer money.

Nonetheless, the indicators described above can be of importance in responding to the threats that may arise from the combination of the above mentioned MMF schemes, as well as for their general understanding.