GLOBAL MONEY FLOWS IN INTERNATIONAL MASS-MARKETING FRAUD PROJECT REPORT

EGMONT GROUP OPERATIONAL WORKING GROUP

APRIL 2015

GLOBAL MONEY FLOWS IN INTERNATIONAL MASS-MARKETING FRAUD

Table of Contents

Introduction: What is Mass-Marketing Fraud (MMF)?

Mass-marketing fraud is a term used around the world to refer to fraud schemes that use mass-communications media – including telephones, the Internet, mass mailings, television, radio, and even personal contact – to contact, solicit, and obtain money, funds, or other items of value from multiple victims in one or more jurisdictions.

MMF was first identified in a handful of countries over 15 years ago. Now it is a global problem, suggesting the need for government officials to work multilaterally to combat this criminal activity. Methods of MMF and its money laundering components are similar to drug trafficking. MMF scams, are perpetrated through mass communications media offshore, usually from a criminal organization. Fraud proceeds, (similar to drug trafficking) are remitted in a different direction to conceal the source. Likewise with drugs, 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 targeting victims in numerous countries on multiple continents, using the advantage of international borders to hinder legislative authorities prohibiting the schemes. Fraudsters can perpetrate their scheme from anywhere in the world, which makes identification difficult and time consuming.

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

Project Objectives and Benefits

The Financial Crimes Enforcement Network (FinCEN) - United States proposed and led this project to compile financial information from interested jurisdictions to determine the flow of money associated with MMF. The financial intelligence unit (FIU) participants in this project are Australia, Canada, Finland, France, Netherlands, Nigeria, the United Kingdom (UK), and the United States (U.S.).

The goals of this project include:

- Establishing indicators of the multiple types of MMF as well as patterns and trends of MMF to help FIUs conduct their analysis of this financial crime **(Phase I)**;
- Compiling specific country experiences of MMF and a compendium of MMF cases **(Phase II)**

Participants' answers to a questionnaire (Appendix), intelligence reports, emails and other data defined the scope of this paper.

International Mass-Marketing Fraud Working Group

The International Mass-Marketing Fraud Working Group (IMMFWG) was formed in September 2007. It consists of law enforcement, regulatory, and consumer protection agencies from Australia, Belgium, Canada, Netherlands, Nigeria, UK, and U.S., as well as Europol. The IMMFWG is a collaborative resource that meets twice annually to exchange intelligence, coordinate cross-border operations to disrupt and apprehend mass-marketing fraudsters, develop strategic projects, and discuss awareness, education, and prevention campaigns for the public. These coordinated efforts address the following types of fraud.

Mass-Marketing Fraud Types

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

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

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.

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. Perpetrators exploit sympathetic causes, legitimate charities' names, and humanitarian or environmental disasters.

Counterfeit Check Fraud Schemes require that the recipient deposit a check or money order into his/her bank account, and then wire transfer a portion of the value of the check or money order back to the sender/fraudster. Fraudsters may send a disbursement as lottery winnings or payment for a high-value item such as a car, commonly using counterfeit checks or money orders to enhance the perceived legitimacy of the transaction. 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.

Emergency Assistance Schemes require immediate financial assistance for bail or emergency medical expenses. A perpetrator poses as a family member or close friend with a request for urgent financial assistance, claiming that the victim's family member overseas (often a college student studying abroad) was arrested or was in an accident.

Employment and Business Opportunity Fraud Schemes 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. 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.

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

Investment Fraud Schemes promise nonexistent monetary awards in exchange for the advance payment of fictitious fees and taxes. This is also known as "boiler room" fraud. Schemes include penny stock schemes and high-yield investment programs. High returns are promised from the purchase of securities, real estate, stakes in oil drilling ventures, coins, gems, and other commodities.

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 target individuals and small businesses.

Mass-Marketing Fraud Schemes Targeting Businesses are fraudulent invoice scams and deceptive solicitations to purchase discounted office supplies, or advertisements in nonexistent business directories or poorly-crafted websites.

Product Misrepresentation Schemes are deceptive offers of goods and services, including credit protection and repair programs, vacations, timeshares, green card application services, dating 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.

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

Romance Schemes: Perpetrators of romance 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 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.

Traditional West African Fraud Schemes: Victims are enticed 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 stolen 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:

- ***Black-money schemes*** solicit victims to purchase special cleansers to remove dye from paper currency that has, for various reasons, been blackened and rendered unusable.
- ***Inheritance schemes*** involve perpetrators requiring victims pay fictitious fees and taxes to claim nonexistent estates of previously-unknown and now-deceased relatives.

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

Identity theft is commonly used to perpetrate MMF, 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.)

An example of an MMF scheme follows:

1. A fraudster sitting in a café in Africa uses the Internet to perpetrate an emergency assistance scheme to defraud a U.S. citizen.
2. The fraudster convinces the victim that his grandson, who is spending a college semester overseas, has been arrested and needs money for legal expenses.
3. The fraudster instructs the victim to send his money (unknowingly) to a fraudster in Asia.

MMF frauds are committed by fraudsters and the illicit proceeds are received by their counterparts in countries on every continent in the world. Fraud networks are designed to perpetrate the activity as quickly and easily as possible. All of this information leads to the question, "Where does the fraud money go?" This question inspired this "Global Money Flow in International Mass-Marketing Fraud" project for the Egmont Group.

Trends and Patterns of MMF

The participants identified the top five frauds, beginning with the most common, as West African (including 419), lottery/sweepstakes, advance fee, employment, and romance. However, the top five fraud types represent only 25 percent of MMF recognized by the FIUs.

Based on the data received, the global money flow related to MMF spans 58 countries on six continents and three regional areas. Total estimates of MMF proceeds are in the tens of billions of U.S. dollars

(circa 2010)[1]. Participating FIUs' data revealed all MMF proceeds identified were funneled to Africa, Asia, Europe, and North America, especially to Nigeria, the UK, and the U.S.

Six of the world's seven continents receive MMF proceeds. Based on the participating FIUs' data, the percentages of countries on each continent receiving MMF proceeds are:

- Africa – 18% or 10 countries
- Asia – 29% or 14 countries
- Australia – 100% or one country
- Europe –36% or 18 countries
- North America – 100% or three countries
- South America – 33% or four countries

- Three regional areas also receive MMF proceeds. The percentages of countries in each area receiving MMF funds are:

- Caribbean – 15% or two countries
- Central America – 29% or two countries
- Middle East – Definition of this region varies. Four countries were involved.

Indicators

Participant FIUs shared the following MMF indicators based on STR data identified during this project. The indicators can enhance the ability of FIUs and the financial industry to recognize MMF proceeds when they are encountered:

- Repetitive and rapid in-and-out transactions;

[1] International Mass-Marketing Fraud Working Group, International Mass-Marketing Fraud Threat Assessment, June 2010

- Multiple transactions to avoid reporting requirements;
- Round sum transactions;
- Use of money machines to avoid human interaction;
- Receipt of wire transfers from entities with no relationship or connection;
- Transfers to or from high risk money laundering jurisdictions outside of business purpose;
- Use of false documentation when transferring funds;
- Vulnerable individuals (elderly) sending money overseas without purpose and using money service businesses;
- Individuals behaving defensively when questioned about money transfers;
- Third party transfers from overseas followed by immediate large cash withdrawals;
- Use of personal account for business transactions;
- Large amount of funds inconsistent with client profile;
- Use of cash couriers;
- Use of multiple MSB's in the same geographical location;
- Large high volume of money transfers through MSBs;
- Credit card Internet transactions;
- Use of Internet-based payment systems like PayPal;
- Sending multiple transactions on the same day to the same beneficiary;
- Sending international fund transfers to high risk money laundering jurisdictions
- Large cash deposits and wire transfers;
- Large number of bank accounts by customers at the same financial institution;
- Cash deposits by 3rd parties;
- Use of various spellings of names and address;
- Use of altered or counterfeit checks; and
- Both large and small value of international fund transfers.

Indicators are not strictly defined as being facilitated by 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. The

threat of violence enables the fraudster to convince the victim they are helpless if they don't comply. This creates a cycle of criminal activity that is difficult to break.

Fund transfers are accomplished through multiple types of transactions. The money can deposited and withdrawn from one or many bank accounts, either in cash or through wire transfers where the account holders use fictitious names; moving cash through MSB's 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 use of identity theft to open accounts or transfer money.

The victim and/or perpetrators that facilitate the money flow as the sender or receiver is difficult to calculate. The use of false identification and the actual number of transactions can be counted. However, tracking actual identification of the victim/perpetrator and funds withdrawn or moved in cash currency can be lost.

Conclusion – Phase I

In the last 20 years, MMF expanded from non-existent to a high-growth criminal industry victimizing people around the world. Data provided by the participating FIUs for this project describe MMF's global reach, common methods of fraud, and the enormity of illicit proceeds. Although we still do not know the full scope or total cost, we now know MMF is a truly international threat with recognizable characteristics and devastating consequences. Working together is the most effective way to combat this crime.

International Mass Marketing Fraud (IMMF) Phase II

Recent investigations of mass-marketing fraud indicate that fraudsters continue to use innovative and sophisticated techniques to request victim payments via cash-based methods, including checks, money orders and paper currency to name a few.

The IMMFWG prepared a threat assessment in 2010 to educate governments and the broader public with an estimation of the nature and scope of the current threat that mass marketing fraud creates around the world.

Indicative of many successful criminal enterprises, mass marketing perpetrators take great care to conceal the origins, beneficiaries, destinations, and uses of their proceeds to hinder law enforcement investigators' efforts to trace and seize the illicit funds.

Jurisdictions have encountered a wide array of assorted fraudulent activities of dissimilar proportions in terms of the number of victims reported and the amount of their losses. Although the types of frauds vary from one jurisdiction to another, similarities exist in the *modus operandi* and how the proceeds are transferred.

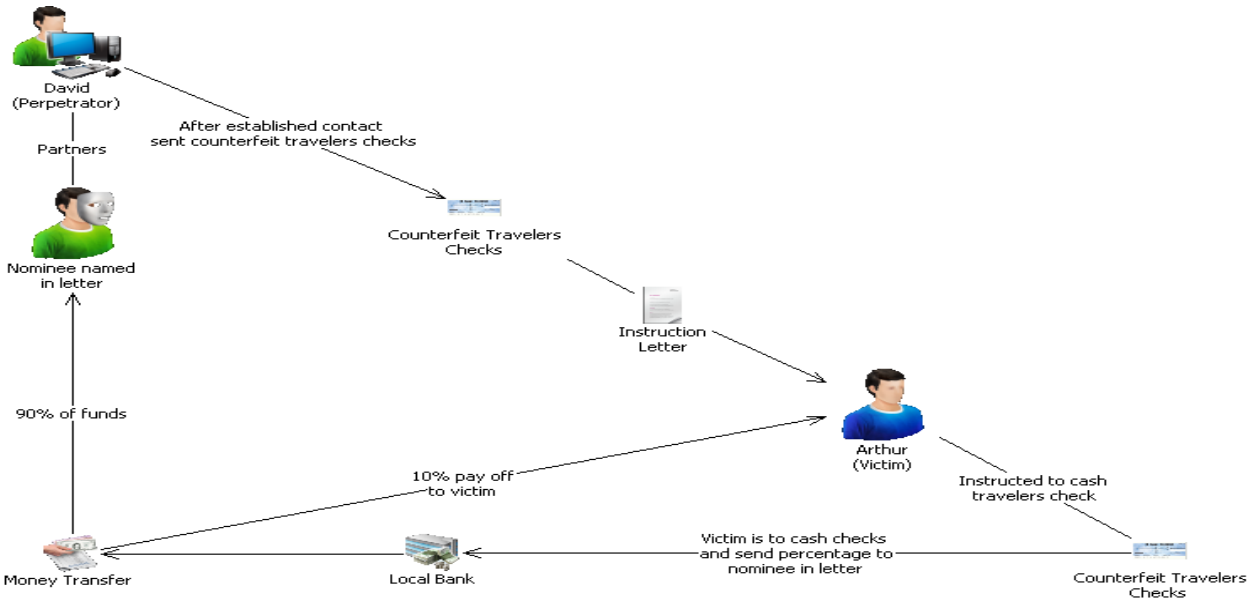
In the close out of Phase II of the Egmont OpWG study of the examination of the flows of money associated with mass marketing fraud, a compendium of global case studies was examined and highlighted the sophistication of the fraudsters' *modus operandi.* Some of these cases are included below and are intended to facilitate jurisdictions' understanding of unfamiliar methods employed by the perpetrators of IMMF.

International Mass Marketing Fraud: Case Studies

Case Study 001: Counterfeit Check Fraud Scheme

An individual made contact with a foreign national via e-mail. Subsequently, he received counterfeit Travelers Checks from a second individual along with a letter of instructions providing details of how to cash the Travelers Checks and disburse the funds. The letter directed the foreign national to present the checks at his local bank for cash and transfer 90 percent to a nominee while keeping 10 percent as a payoff for performing the transaction.

Fortunately, the bank practice did not allow for immediate cash payout. The bank will routinely accept checks on deposit and make the cash available only after verification is received from the issuer's bank. The foreign national was unable to receive any funds against the counterfeit Travelers Checks and ultimately the checks were confiscated and turned over to law enforcement authorities for further investigation.



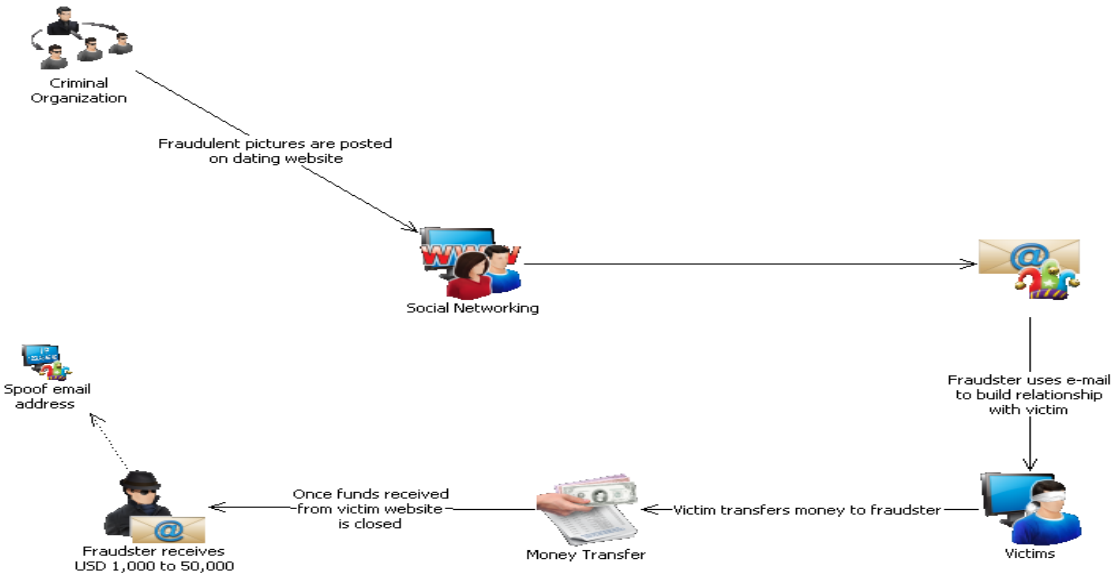
Relevant indicators:

- Use of email to contact victim.
- Use of counterfeit Travelers Checks to receive a payout.
- Request victim to use personal bank account to cash Travelers Checks.
- Letter of instructions how to disburse cash.

Case Study 002: IMMF Advanced Fee Fraud through the Internet

A crime syndicate posted pictures of foreign females on dating websites to lure male victims looking for female companionship via the internet. Once the victims established contact through email and regular conversation, the scammers began to request money for various reasons. Some of the reasons given were the need for "up-front" funds to purchase a plane ticket for a face-to-face meeting, or financial hardship, life crisis, or something similar. The requested amounts of money ranged from $1,000 USD to $50,000 USD. Once the funds were transferred, the scammers would discontinue all contact and remove images from the website.

Data revealed the network used internet payment systems (IPS) to process credit card transactions that allowed the network to receive the illicit funds from the victim subscribers. The transactions conducted were paid to a fictitious company and subsequently forwarded to a nominee beneficiary customer, usually the scam operator.

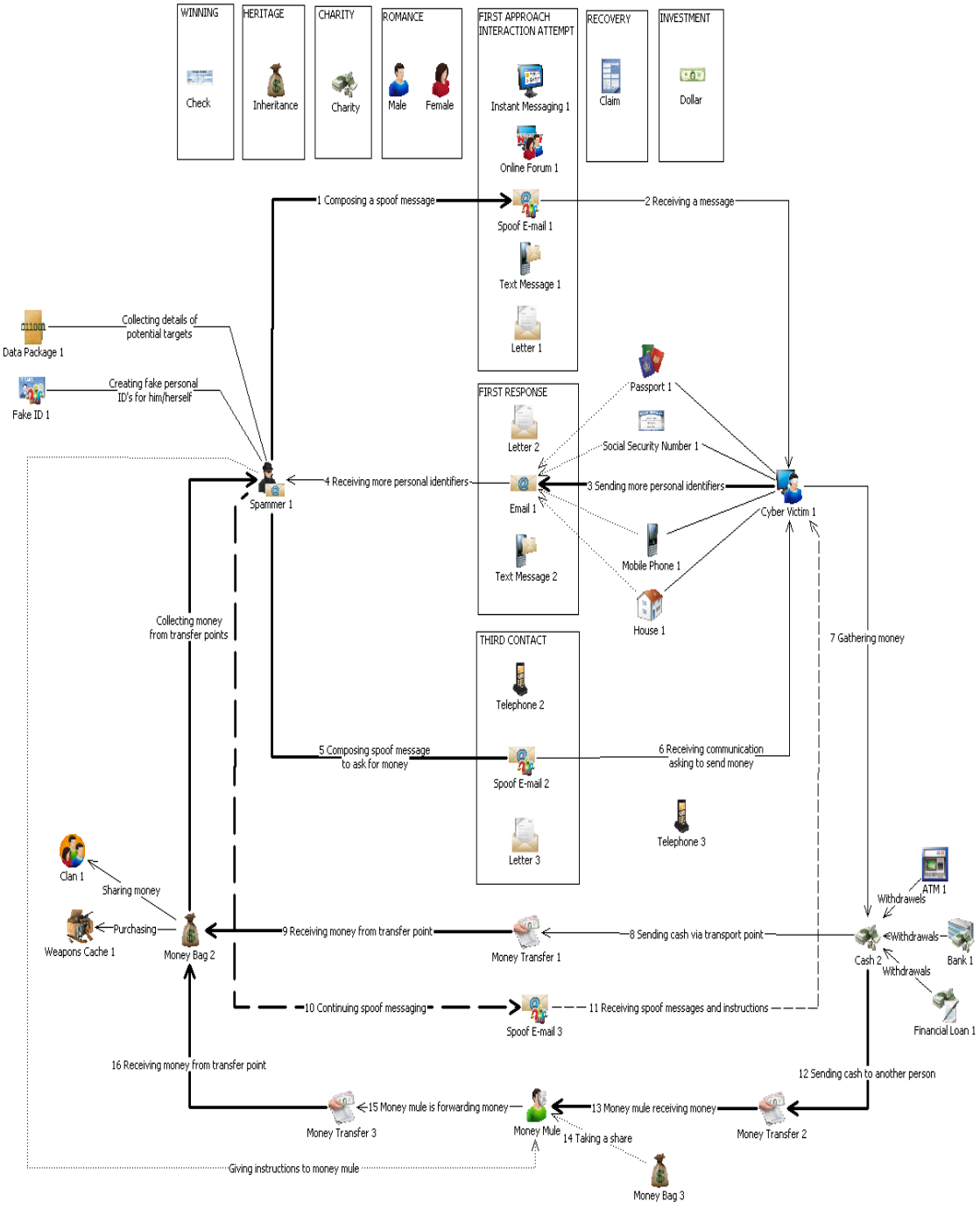


Relevant Indicators:

- Use of social websites to identify companion.
- Use of romance emails and attractive photos to lure victims.
- Use of psychology to establish relationship and gain trust from victims.
- Perpetrator uses various excuses to get money from the victims once relationship is formed. Once the fraudsters receive the funds the website is shut down and images are removed.

Case Example 003: Link Analysis Chart International Mass Marketing (IMMF) Fraud Behavior

Provided below is an IMMF link analysis chart depicting the various phases of IMMF activity. In the chart, several different IMMF schemes are depicted.



Case Example 003: Link Analysis Chart Mass Marketing Fraud Behavior

The highlighted numbers below correspond with the numbered nodes on the link chart above:

Mass Marketing phishing phase

1&2. The fraudster composes a spoof message to obtain personal data from the cyber victim.

3&4. The cyber victim provides the perpetrator with his/her personal identifying information.

Mass Marketing money begging phase

5&6. The fraudster composes a spoof message to ask for money.

7,8&9. The cyber victim transfers personal funds to the fraudster as requested.

10. The fraudster continues to ask for money, composing different types of spoof messages.

Mass Marketing money mule phase

11&12. The cyber victim is sometimes guided to send money to other people.

13,14&15. Often, recruited money mules do not know what the fraudulent scheme entails. The mule sets the instruction from the fraudster. Several money mules can be assigned to one victim.

16. The fraudster may collect funds from transfer points.

Case Example 004: Advanced Fee Lottery Scheme

In early 2009 a foreign authority received a suspicious transaction report (STR) from a securities dealer on a particular customer (X) reporting that he had received a large wire transfer of $15,650 USD. From this amount, transfers were made to the accounts of two other customers. Simultaneously, another STR was filed by a related financial institution indicating that all three persons were making frequent cash deposits to their accounts.

Financial queries revealed that a money transfer agency had also submitted multiple STRs on Customer X and one of his associates indicating that they were receiving money transfers from many persons in the USA.

One of the reasons provided by Customer X for the money transfers was that his aunt had sent him the money to assist in purchasing a boat.

In June 2009, a disclosure (case file) was prepared by the foreign authority and disseminated to the necessary office within the police unit assigned to investigate cases generated from suspicious and threshold transaction reports.

In September 2010, the securities dealer again filed STRs on two other wire transfers totalling $70,000 USD credited to the account of Customer X's mother.

In October 2010, the same securities dealer contacted the foreign authority, requesting consent to pay out funds of over $107,000 USD to Customer X and his mother. These funds included the $70,000 USD that were previously reported but had been held by the financial institution. The foreign authority immediately contacted law enforcement officials in the state of the sender. It was ascertained that the sender was an elderly woman who had actually taken a loan from her credit union to source funds that were sent to Jamaica. Based on this information, the foreign authority refused consent to pay out the funds to Customer X and instructed the securities dealer to return these funds to the sending financial institution in the USA.

The securities dealer and the related financial institution then closed all accounts in the names of Customer X and his mother. However, wire transfers were then sent by the same senders and others to other associates of Customer X.

In September 2011, another securities dealer filed a STR on Customer X noting that he had opened new accounts consequent to his accounts being closed by the first securities dealer. The reports filed by the second securities dealer were similar - multiple wire transfers totalling over $91,000 USD between April

and August 2011 from numerous senders including the elderly sender to whom funds had previously been returned. The funds were withdrawn in cash as soon as the accounts were credited.

This new information was disseminated to the appropriate authority as a Note to File.

The foreign financial investigators sought the assistance of U.S. agents to obtain statements from victims. This proved to be particularly challenging as although U.S. agents were helpful and willing to assist, the statements had to be produced in a particular format and obtained in accordance with international legal procedures to be acceptable in the local courts. After several attempts, two statements were received from victims.

Victim A in the U.S. stated that she was contacted and told that she had won $1.5 million USD in the lottery and that she needed to wire $200 USD to collect her prize. She was then told to wire other amounts. Eventually, she ran out of funds. She was then instructed to collect funds from Victim B (the elderly woman) in U.S. to forward to the other country. This she did, collecting $275,000 USD from Victim B which was then sent via wire transfers to Caribbean. The statement of Victim B in the U.S. corroborated the statement of Victim A in a different state in the U.S.

Production Orders were also served on the financial institutions that had conducted transactions for Customer X. Analysis of these transactions revealed that Customer X and his mother had received over $324,000 USD from possible victims in the USA.

Customer X and his mother were arrested in May 2012 and the following charges were laid against them:

1. Obtaining money by means of false pretence
2. Engaging in transactions involving criminal property
3. Transfer of criminal property
4. Acquisition, use and possession of criminal property

They have already appeared in court twice. The next hearing will be in July 2013.

Relevant Indicators:

- Frequency of the transfers
- Size of the transfers
- Number of senders who were sending to multiple recipients
- Location of the recipients
- Use of multiple addresses

- Age and occupations of the recipients
- Purpose of the transfers

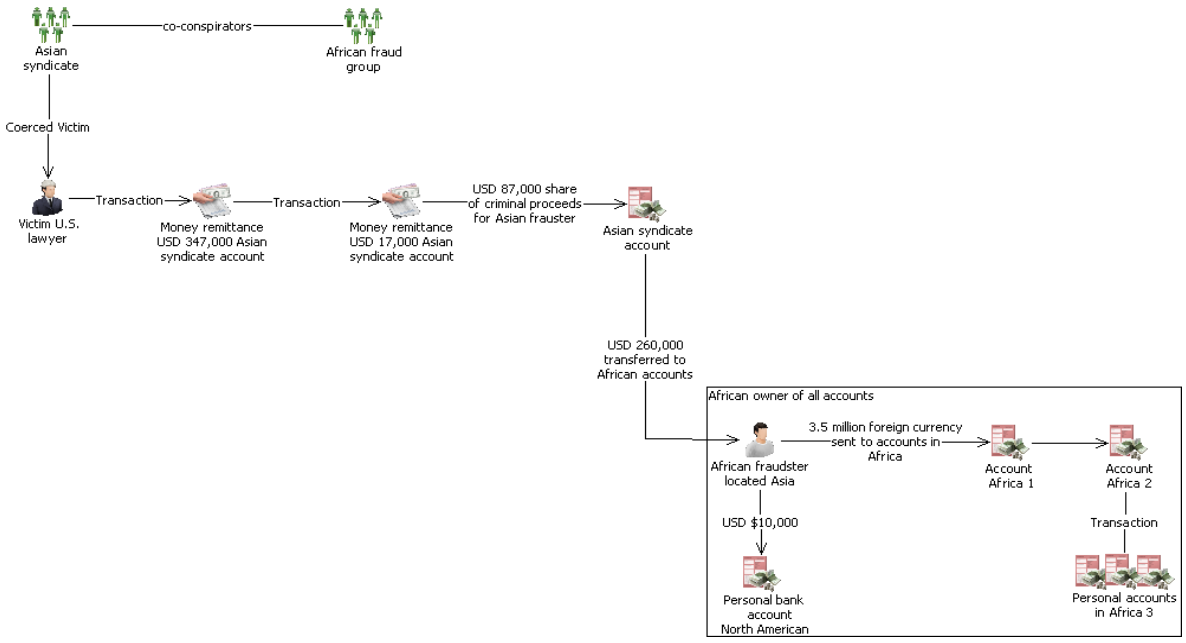
Case Study 005: Transnational Organized Crime and Mass Marketing Fraud

A U.S. lawyer was coerced by a member of a well-known Asian syndicate to transfer large sums of money to a bank account at a local Asian bank. Once deposited, nearly three quarters of the criminal proceeds were transferred to an African national who subsequently sent those funds to another country and Africa.

The Asian syndicate member and the foreign national from Africa were arrested for possession of criminal proceeds. Asian law enforcement believes that the African national is a member of an international fraud group, and has concerns about the perpetrators' future collaboration with criminal organizations operating in Asia.

The money flow is as follows:

- The U.S. victim wire transferred $347,000 USD to the Asian syndicate account and sent an additional $17,000 USD the next day.
- $260,000 USD was wire transferred from the syndicate account to an African local.
- The Asian perpetrator took his share, $87,000 USD.
- The African perpetrator wired $10,000 USD to a bank account in another country.
- The African perpetrator then wired $250,000 USD to one of his bank accounts in Africa, exchanging the proceeds to 3.5 million in foreign currency. The perpetrator then transferred funds to another account in Africa, subsequently sending 3.2 million in foreign currency to four individuals within 10 days.



Case Study 005: Transnational Organized Crime and Mass Marketing Fraud (cont'd)

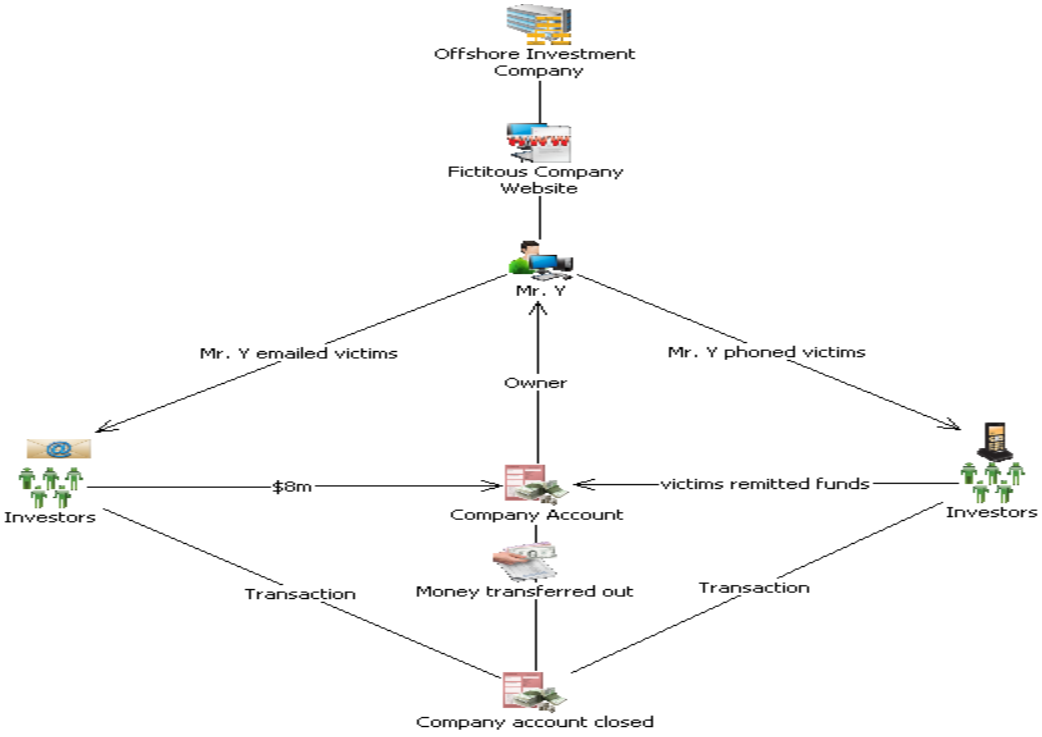
Relevant indicators:

- Two syndicates working together
- Coercion of victim abroad to wire funds
- Multiple accounts used to move funds and disguise money trail

Case Study 006: Investment Fraud Offshore Company

A foreign national, Mr. Y, came to Asia and set up an offshore investment company. Subsequently, Mr. Y opened a bank account under the company's name to support business operations. Mr. Y created a fictitious website to lure potential victims advertising the investment company's background and overall achievements. Information on the website boasted of the company's strong investment team and their ability to assist clients with stock investments that yield a high rate of return in a short period of time. Mr. Y began to contact clients worldwide by telephone and email to persuade them to invest funds in stocks.

As a result of Mr. Y's efforts, a number of clients remitted $8 million to the investment company's bank account. After the receipt of funds, the account balance was transferred out and the account closed. Two of the fraud victims came forward and made claims against the company aiding in the identification of the suspect. The case is pending litigation.

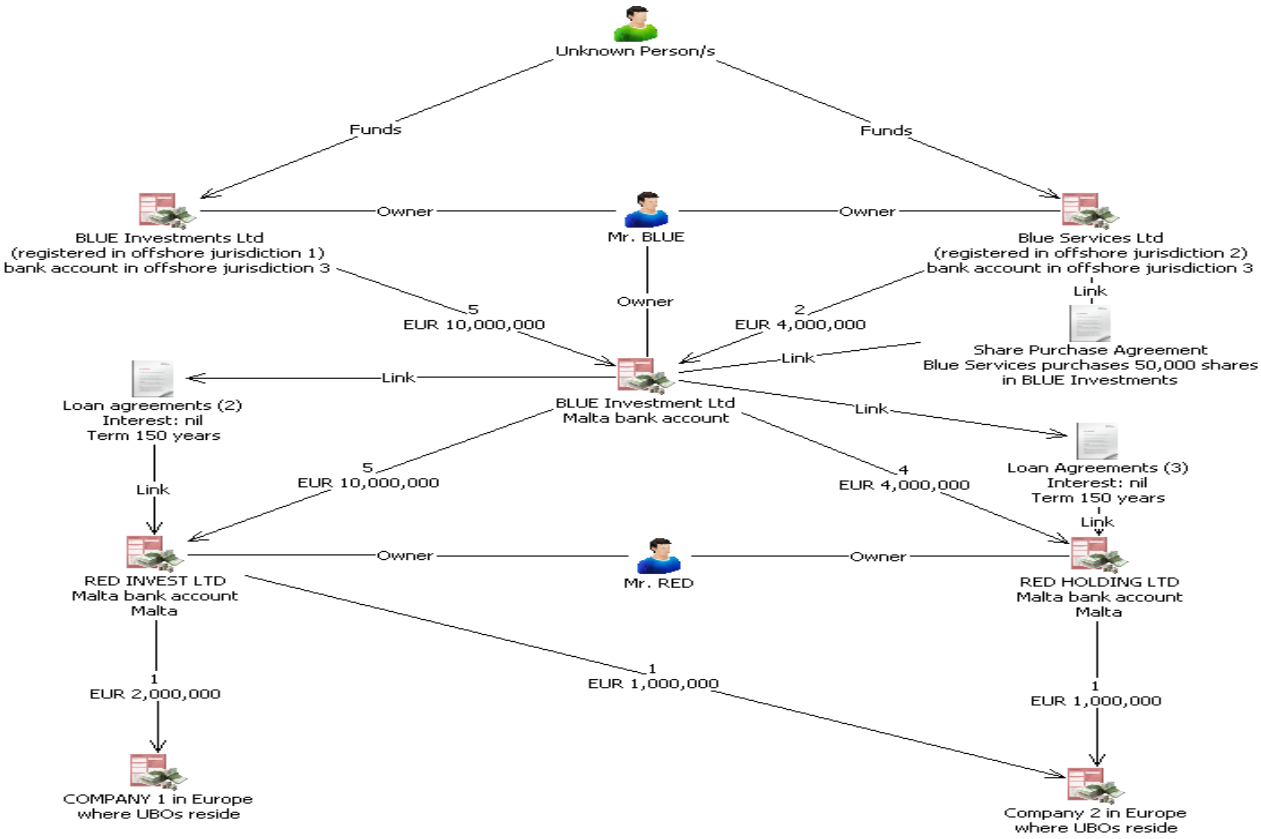


Relevant Indicators:

- Use of Offshore Company
- Contact victim by email and telephone
- Transfer funds out of business account to disguise money trail
- Close company account upon receipt of funds

Case Study 007: Ponzi scheme (High Yield Investment)

A suspicious transaction report (STR) contained adverse information on clients Mr. Red and business partner Mr. Blue. Both resided in Europe, maintained bank accounts, and owned companies registered in a particular country. Information revealed Mr. Red had a conviction associated with an international stock manipulation scheme. Allegedly, he issued false press releases and misrepresented his company's business dealings by sending attractive promotional mailings to over two million U.S. recipients. Information indicates Mr. Red unloaded more than a million dollars in fictitious company stock on unsuspecting investors. Following this campaign, the stock price doubled and the trading volume spiked more than 1,200%. The perpetrators sold the inflated stock holding for profits in excess of $10 million.

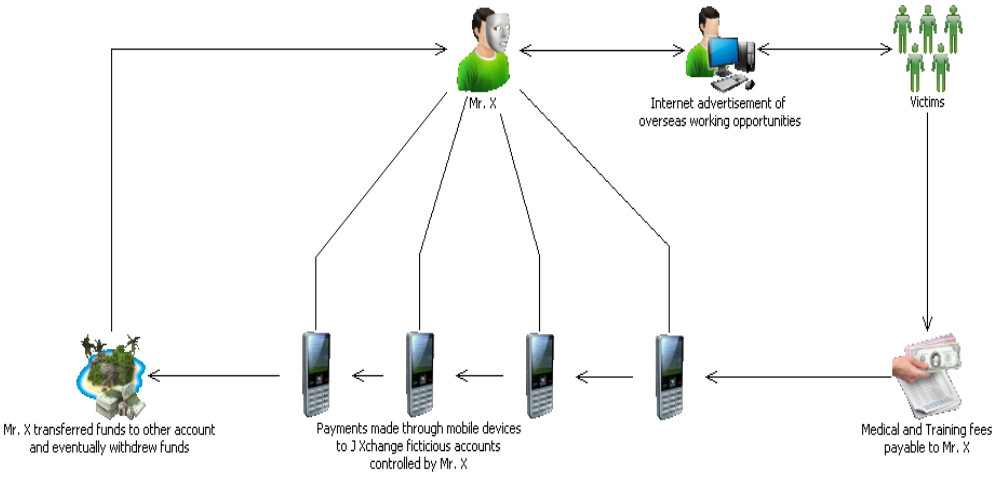


Relevant Indicators:

- Use of offshore shell company
- Investors remitted investment funds to offshore bank account
- Investment funds were further disposed by remittances to other jurisdictions
- Immediate withdrawal of funds remitted to the account

Case Study 008: MMF Scheme involving the Use of Mobile Payment System

Mr. X posted advertisements of overseas work opportunities on the Internet. He used several fictitious names, pretending to be a legitimate recruiter or employer. Applicants were misled, offered overseas employment and required to pay medical and training fees ranging from Php 3,000 to Php 45,000. Payments were made and received through a mobile phone payment system to a company "J Xchange." Mr. X established several accounts under falsified names where unsuspecting victims were directed to send payments. Upon receiving the victim's deposits, Mr. X wire transferred the funds multiple times, to various accounts, and eventually withdrew the funds in cash.



Relevant Indicators:

- Use of Internet to entice victims
- Use of mobile payments systems
- Use of false identification to open mobile payment accounts and conceal the account holder's identity
- Use of multiple payment accounts to complicate the fund flow

Case Study 009: Investment Fraud

An Asian authority received a suspicious transaction report (STR) identifying a company founded in May 2010 by Mr. W. The listed company directors, Mr. X and Ms. Y, were not only business partners but also romantically involved with one another. On this occasion, the company accountant Ms. Z and Ms. Y withdrew large sums of cash from the company account on two consecutive days. The consecutive withdrawals raised suspicion among bank officials, suggesting the intent to close the company account discreetly.

The Asian police already had an active investigation on the subjects. One of the investors complained to authorities of the company's failure to pay capital and interest on schedule. The matter was investigated by reviewing company accounts and interviewing employees. This quickly raised suspicion among Mr. W and his accomplices, and Mr. W fled the country while Mr. X and Ms. Y were arrested attempting to flee the country.

The investigation revealed sales fraud that had illegitimately absorbed funds of up to $83.3 million USD from individuals in Asia for nearly three years. Investors were promised a monthly income of 30 percent for their investment in a fraudulent scam related to massage arm chair rentals purportedly placed in hotels and shopping malls in Japan. The company also guaranteed a secure return on investments within 10 months and profits of up to three times the original investment within three years.

The authorities executed a search warrant and seized $400,000 USD found at the company headquarters. The authorities uncovered $3.1 million USD and with the help of law enforcement placed a freeze on the account. A total of $5.5 million USD of the illicit proceeds were seized from another account, and $3.3 million USD was found transferred to other accounts owned by Ms. Y.

In April 2012, Mr. W and Mr. X were prosecuted and sentenced to 18 years in prison. Ms. Y was prosecuted and sentenced to 16 years imprisonment. The accountant, Ms. Z, was prosecuted and sentenced to 7.5 years in prison for her role in the fraud.

The bank did a very good job in implementing the "know your customer" (KYC) requirements and was familiar with the relevant employees and business framework of the fraudulent company. This allowed for rapid detection of illicit behavior, facilitating a STR filing and restraint of pertinent funds in collaboration with the authorities in Asia. The authorities in Asia provided positive feedback to the financial institution acknowledging their employees who were involved, and case information was provided to the partner authorities for action they deemed appropriate.

Relevant indicators:

- Company is new founded - within last two years

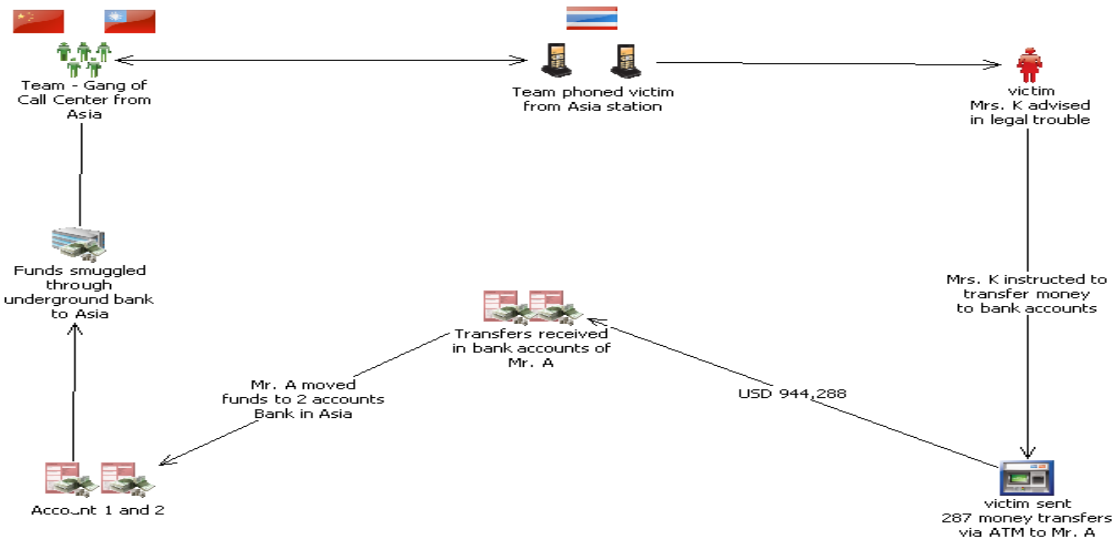
- Company officers are romantically linked
- Guaranteed large and returns for investments quickly
- Illicit funds transferred to offshore account

Case Study 010: Fraudulent Criminal Charges to Collect Fees

A syndicate based in several parts of Asia set up operations in another part of Asia with the intention of defrauding victims by phone. The caller identified himself as the Secretary General of the Anti-Money Laundering Office. The victims were coerced into believing that they had been unwittingly involved in a drug trafficking operation. In an effort to avoid legal action, the victims were instructed to transfer funds to several different accounts at a bank in Asia. A victim, Mrs. K, was persuaded and executed 287 money transfers amounting to $944, 288 USD into the fraudster's accounts via an automatic teller machine (A.T.M.).

Financial investigations revealed that all of the ATM deposits were subsequently moved to several different accounts of an Asian citizen, Mr. "A." To avoid detection, the illicit proceeds were discreetly smuggled out of the country via an underground banking system, destined for two locations in Asia. This activity was intended to complicate the money trail and disguise the financial flow, thus confusing the investigative efforts of authorities.

There were 100 victims in this IMMF case with damages amounting to $1,647,847 USD. Since January 2012, the assets of Mr. A and his accomplices have been temporarily seized by authorities in Asia.



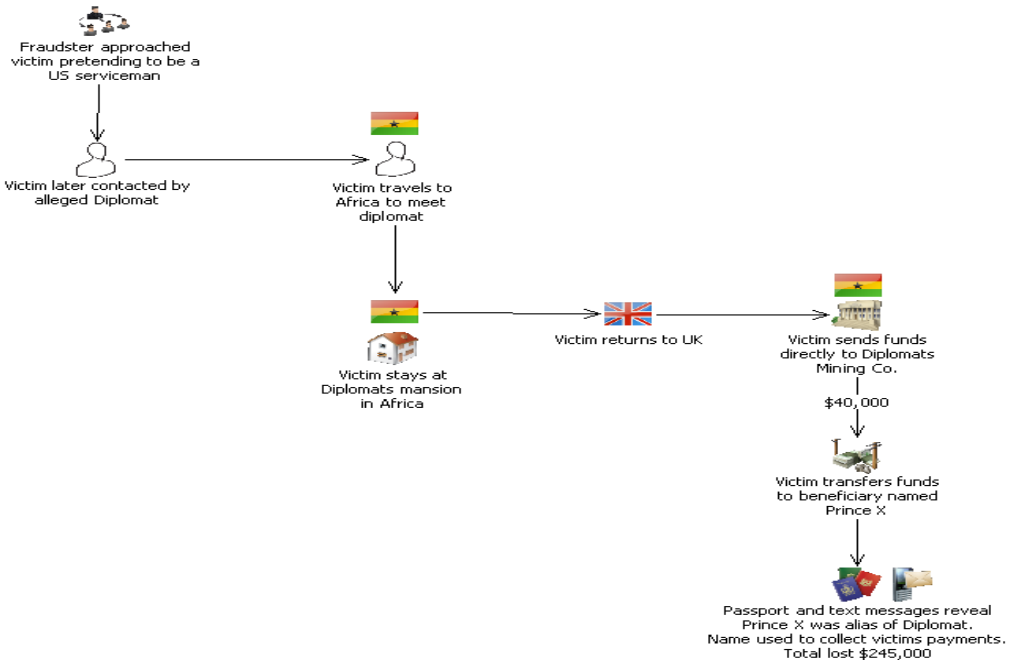
Case Study 010: Fraudulent Criminal Charges to Collect Fees (cont'd)

Relevant Indicators:

- Fraudsters set up call center outside of their jurisdiction
- Use of telephones to facilitate fraud
- Fraudster identified themselves with official organization to persuade victim
- Use of ATM, multiple bank accounts, and underground banking system avoid detection and disguise illicit money flow

Case Study 011: Romance Scam

A female victim, 51 years of age, lost 245,000 UK, alleging she was approached on a dating website by a person purporting to be an American serviceman. Subsequent contact alleged the caller to be a diplomat, and she agreed to travel to Africa as a houseguest of the fraudster. After establishing a romantic relationship, the victim sent the fraudster 40,000 UK payable directly to his mining company. The victim subsequently received documents to support the fraudster's UK visa application. The victim sent additional money via wire transfers to a beneficiary with a different name than the fraudster. The beneficiary's name was identical to one of the names found on the fraudster's many passports recovered at the time of arrest. Information indicates the fraudster used his alias as identification to collect the victim's payments.



Case Study 011: Romance Scam (cont'd)

Relevant indicators:

- Use of social engineering coercion
- Use of multiple passports with several aliases
- Request for funds after romancing the victim

Case Study 012: Caribbean Lottery Scam of the Elderly

In early 2012, an elderly victim in the U.S. received a phone call from someone in the Caribbean claiming to represent Publishers Clearing House. The caller congratulated the victim and told him that he had won a car and a large sum of money. He assured the victim the call was genuine, and that the victim would merely need to pay a $500 USD transfer fee to have the vehicle shipped to him. Following this phone call were several other calls from people claiming to be from the Nevada Lottery Commissioner's Office and the Better Business Bureau further reassuring the victim that his "win" was legitimate.

At some point, not long after the initial few calls, a woman called and spoke kindly to the elderly victim and began to ask him questions about what he would do with the money. She befriended the victim and began to build a friendship with him over the phone. She claimed to be the secretary to the chief executive officer of "Mega Buck," a company that handles prizes for Publishers Clearing House. She gave the victim instructions on where to send the money. The elderly victim was told not to tell anyone

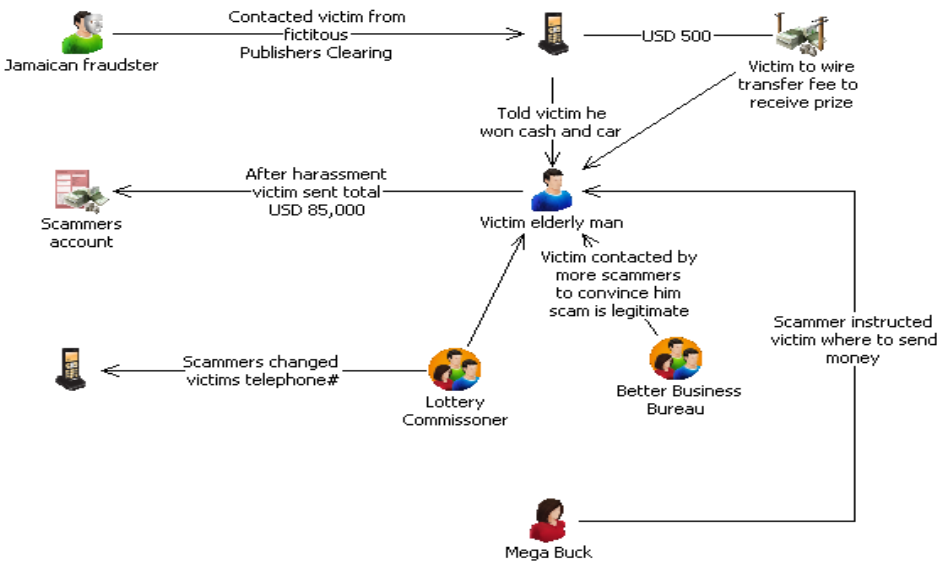
in his family and to let his win be a surprise. The phone calls became more frequent and intimidating, and the victim began to send money on several occasions for different reasons.

The victim's family became frantic after telephoning the victim on several occasions and being unable to reach him. The fraudsters had obtained so much personal information from the victim that they changed his telephone number without his knowledge so that the victim could only receive telephone calls from the fraudsters. The victim's family contacted the U.S. authorities who informed the family that this was a scam. The victim continued to talk to the female scam artist without the family's knowledge as he was convinced she was honest and he trusted her. The family of the victim reconciled his bank account and found that the victim loss in excess of $85,000 USD. When notified, the family reports that the elderly victim was visibly shaking, pale and speechless after realizing he was conned and could never recover any of those funds.

Relevant indicators:

- Elderly victim lived alone
- Several scammers contacted victim simultaneously assuring legitimacy of fraudulent winnings
- Female scammer coerced victim and gained his trust
- Scammers changed the victim's telephone number to isolate him receiving calls only from the scammers using pressure tactics and harassment to send funds as requested

Case Study 012: Caribbean Lottery Scam of the Elderly (cont'd)



Case Study 013: Fraudsters Collect Fees through Fraudulent Mailings

A U.S. federal judge has temporarily halted a European based operation that allegedly tricked small businesses and non-profits into collectively paying millions of dollars to be listed in an online directory in which they had no interest in being listed and for which they did not understand that they would be charged. U.S. authorities are seeking to permanently halt the alleged scam and require the defendants to refund the fees.

According to authorities, the scammers send mailings to retailers, home-based businesses, local associations, and others who attend trade shows. The mailings mention a specific trade show or exhibition and are designed to appear as though they are merely asking the recipient to update and check the accuracy of information for the "exhibitor's directory" for the named trade show or exhibition.

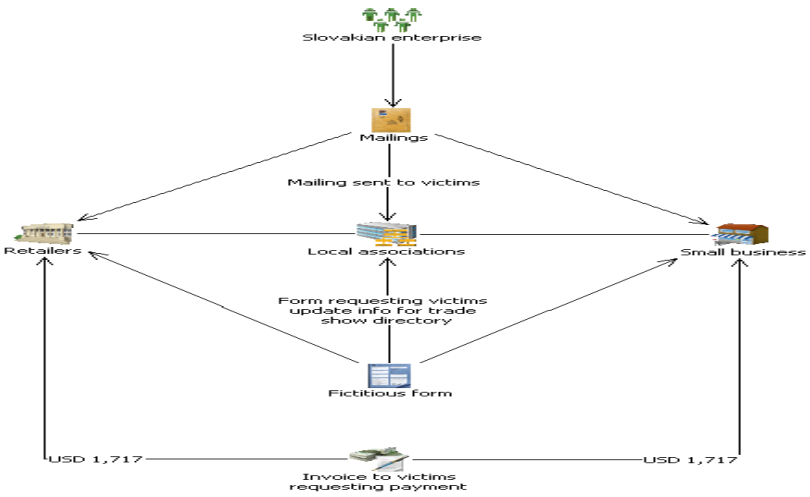
Allegedly, the mailings include a form stating that the recipient's basic information has been listed in the directory for free, and instructing them to confirm its accuracy or make corrections on the form. The form falsely suggests that the parties have a preexisting business relationship and that the directory listing is related to the recipient's participation in the named trade show or exhibition. Many recipients do not notice a statement buried in fine print at the bottom of the form indicating by signing and returning the form, they agree to pay the defendants $1,717 USD per year for three years. Often, the person who returns the form is not even authorized to enter into contracts for their employer.

According to the complaint long after the form is signed and returned, and the defendants' 10-day cancellation period has expired, the defendants send an invoice demanding payment of $1,717 USD to a European bank account. Those who challenge the invoice are told the order cannot be canceled. Late payment notices follow with added late fees which some organizations pay just to end the harassment.

It was found that this enterprise used a mailing house located in the USA to send forms primarily to U.S. recipients. Evidence shows that they continue to do business in 26 other countries around the world. Relevant indicators:

- Mailings sent to retailers and small businesses.
- Mailings pretended to update business information for a trade show directory.
- Buried in fine print were hidden fees.

- Victims were invoiced for fees and late charges incurred if not paid.
- Fraudulent enterprise was dismantled in Austria and perpetrators agreed to close out business; business operations continued in multiple countries around the world.



Appendix - Fact-Finding Questionnaire Related to Mass-Marketing Fraud

1. Which jurisdiction does your FIU represent?

For the timeframe of January 1, 2006 through June 30, 2011, please provide the following information:

2. Has your FIU analyzed or supported cases related to mass-market fraud?

3. Has your FIU prepared a study related to mass-marketing fraud? If so, will you share your results with other Egmont members?

3.1 If your FIU has not prepared a study or analyzed cases on mass-marketing fraud, does your FIU have any financial information related to mass-marketing fraud?

4. If the answer to questions 2 or 3 is yes, what type of mass-marketing fraud did your FIU detect? Please list mass-marketing fraud types.

4.1 If you are unsure, the following is a list of typical mass-marketing fraud schemes:

- Lottery, Sweepstakes or Prize
- Loan
- Credit Card
- Grant
- Product or Merchandise
- Investment (including securities, high-yield, and penny stock)
- Charity
- Advance Fee
- West African (including black money and 419 schemes)
- Inheritance
- Assistance
- Recovery
- Employment
- Work at Home
- Mystery Shopper
- Pyramid
- Auction
- Overpayment
- Invoice
- Web Site
- Romance
- Service
- Business
- Other - Please specify: _____

5. What are the primary financial or non-financial institutions where illicit proceeds from mass-marketing fraud detected in your jurisdiction?

Please check all that apply:

____ Financial institutions

____ Money Service Businesses

____ Casinos

____ Informal Value Transfer System

____ Customs and Border Control

____ Other – Please specify _____

5.1 Does your FIU have STRs related to mass-marketing fraud?

6. Does your FIU collect information regarding cross-border wire (electronic funds) transfers? If so, do you have wire (electronic funds) transfer information related to mass-marketing fraud?

7. In relation to mass-marketing fraud, is your jurisdiction a victim (person or businesses losing money to mass-marketing fraud) or perpetrator (committing the frauds themselves) or both? Please check all that apply:

__ Victim __ Perpetrator

7.1 Do you have any comments on mass-marketing fraud in your jurisdiction? If so, please explain:

_____
_____
_____