The United States Postal Inspection Service Presents

Mass Marketing Fraud Schemes:
How, Why, and What To Do For Victims

National Adult Protective Services Association Conference 2016

Introduction to the United States Postal Inspection Service

"The mission of the U.S. Postal Inspection Service is to support and protect the U.S. Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail."

U.S. Postal Inspectors are federal law enforcement officers who carry firearms, make arrests, execute federal search warrants, and serve subpoenas. Inspectors work with U.S. Attorneys, other law enforcement, and local prosecutors to investigate cases and prepare them for court. Inspectors throughout the country enforce roughly 200 federal laws related to crimes that adversely affect or entail fraudulent use of the U.S. Mail, the postal system, postal employees, and customers. U.S. Postal Inspectors investigate a variety of criminal activity, including but not limited to identity theft, mail theft, prohibited mailings, child exploitation, dangerous mailings, and mail fraud.

For more information, visit https://postalinspectors.uspis.gov/.

Quick Facts about Mass Marketing Fraud

- During the 2015 calendar year, the Federal Trade Commission's Consumer Sentinel Network (CSN) received over 3 million complaints. Over $1.2 million complaints were fraud related and involved customers paying over $765 million to fraudsters. The median amount paid per customer was reported as $400.00.

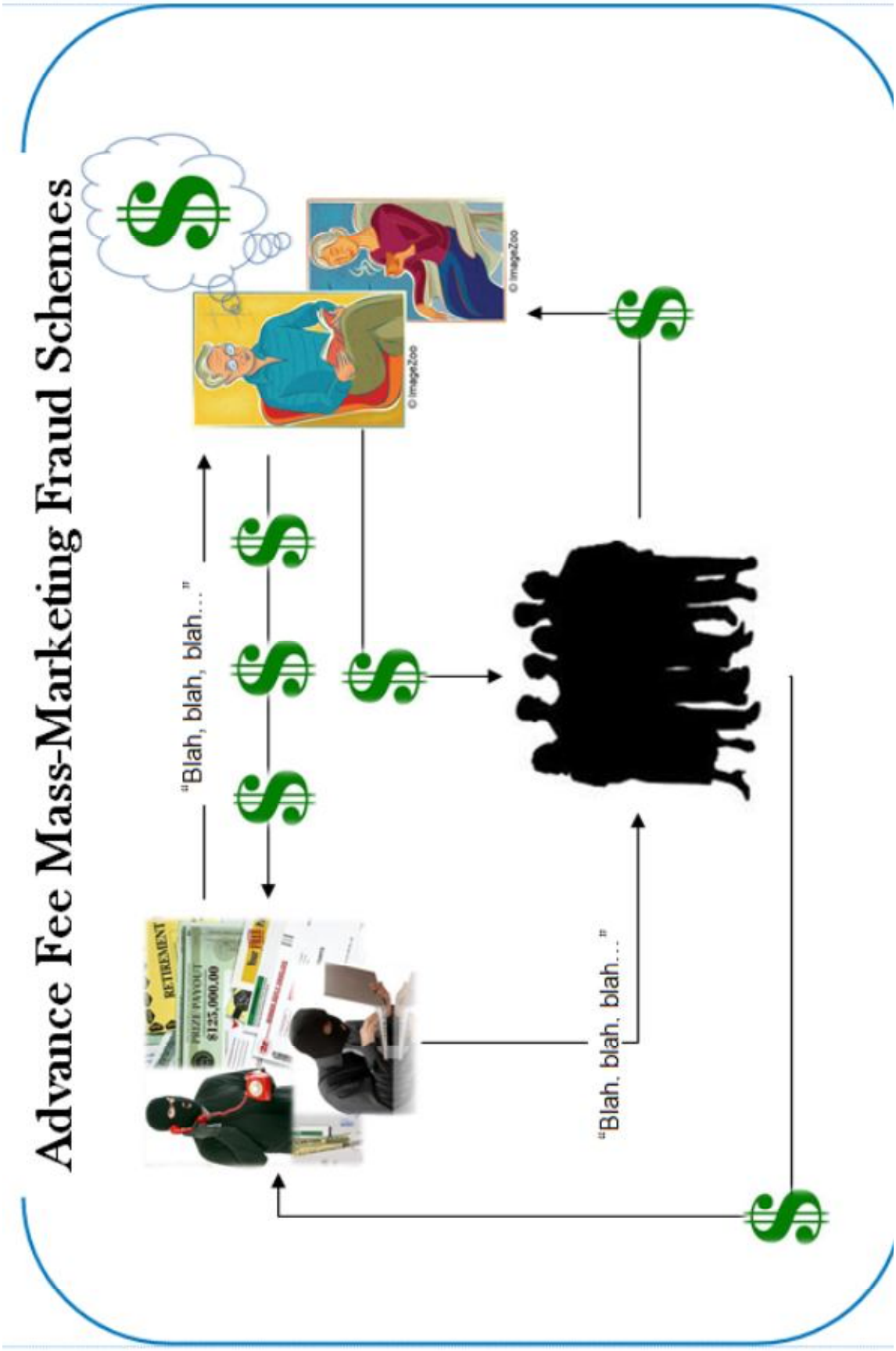
  Federal Trade Commission. *Consumer Sentinel Network Data Book for January – December 2015*. February 2016.

- Lottery scams are an estimated $30 million annual industry in Jamaica.

  Testimony of Corporal Kevin Watson during USA v. Sanja Williams trial, May 2015.

- "Jamaican scammers make as many as 30,000 telephone calls each day to the United States telling people that they have won a non-existent lottery."

  Steve Weisman. *Jamaican lottery scams often start as 876 calls*. USA Today. February 21, 2015.


Advance Fee Mass-Marketing Fraud Schemes
"Blah, blah, blah..."
"Blah, blah, blah..."
RETIREMENT
PRIZE PAYOUT
$125,000.00
© ImageZoo
© ImageZoo

Common Mass-Marketing Fraud Schemes

Advance-Fee Fraud Schemes use solicitations that entice victims with improbable promises of enormous wealth in exchange for upfront 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.

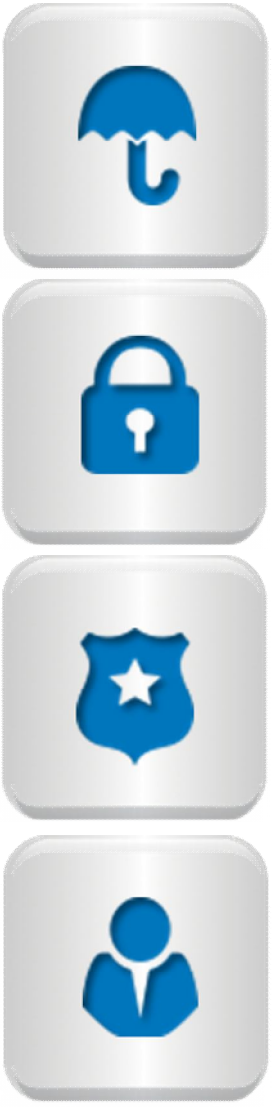
Counterfeit Check Fraud Schemes require that the recipient deposit a check or money order into his/her bank account, and then wire transfer a portion of the value of the check or money order back to the sender/fraudster. Fraudsters may send a disbursement as lottery winnings or payment for a high-value 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 ("Grandparent") 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.



Information adapted from "Global Money Flows in International Mass-Marketing Fraud (Project Report–Phase I)," Egmont Group, July 2012.

Common Mass-Marketing Fraud Schemes, Continued

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.

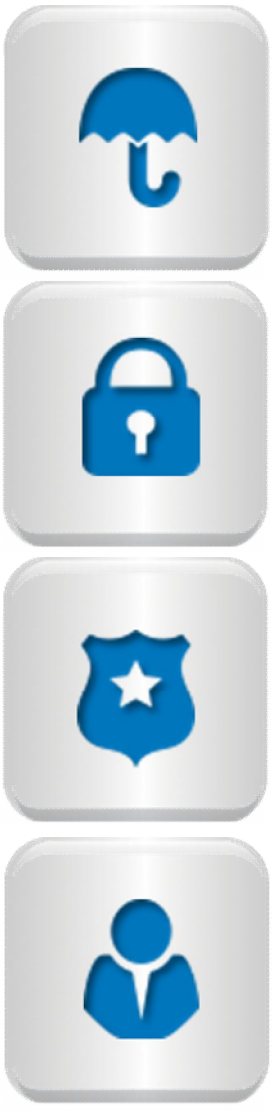
Romance Fraud Schemes target users of Internet dating and social networking sites by feigning romantic interest, securing victims' trust and affection through regular intimate conversations and exchanges of gifts, and then exploiting the relationship to fraudulently obtain money and valuable merchandise. 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 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 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.

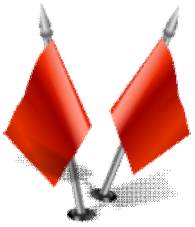
Information adapted from "Global Money Flows in International Mass-Marketing Fraud (Project Report–Phase I)," Egmont Group, July 2012.

Where to Report a Fraud Scheme	How?
Identity Theft Resource	Www.IdentityTheft.gov
General reports of fraud? Anti-Fraud Hotline	 1.855.303.9470 www.aging.senate.gov/fraud-hotline
Telephone or online fraud scheme? Federal Trade Commission Internet Crime Complaint Center	 877.FTC.HELP or www.ftccomplaintassistant.gov www.ic3.gov
Mail fraud scheme? United States Postal Inspection Service	 877.876.2455 or www.postalinspectors.uspis.gov
Scheme involving use of Green Dot MoneyPaks? MoneyGram? Western Union?	 866.795.7597 800.MONEYGRAM or 800.666.3947 Fraud Hotline: 800.448.1492



Mass Marketing Fraud Schemes: How, Why, and What To Do For Victims
NAPSA Conference 2016

Red Flags of Victimization



If it sounds too good to be true, it probably is!

Working with a stranger

No time to make a decision

Secrecy

Great trust in a new friend

Fast money transfers

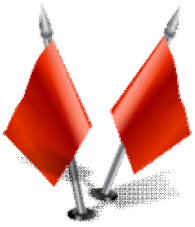
Changes in behavior or routine

Strangers showing up at the residence

Unknown individuals being added to utility or other accounts

Recent food or flower delivery as a surprise to the recipient

Car dealership staff, tow truck drivers, couriers, or realtors visiting unannounced



The money has been sent. What can I do now?

Was the cash/check/wire/reloadable prepaid card sent recently? If yes, then:

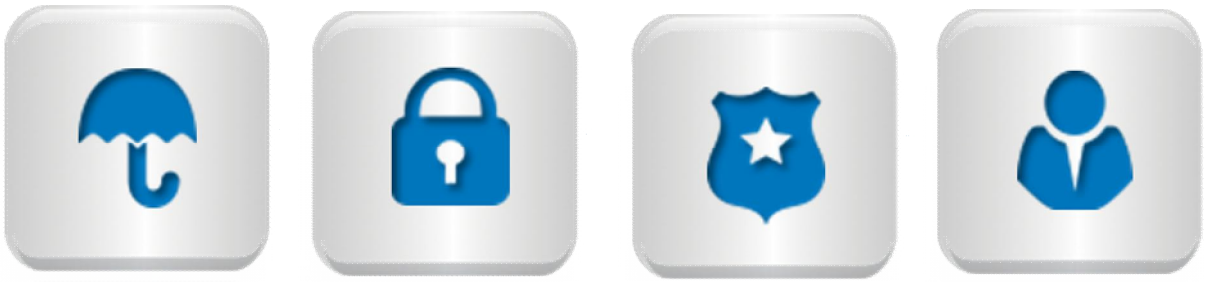
- **U.S. Mail**: Call the U.S. Postal Inspection Service ASAP to attempt to intercept (stop delivery) of the mailing. Provide the address and tracking number to General Analyst Sharon Miller at 877.876.2455. If a check was sent, consider contacting the bank to place a stop payment on the check.
- **Reloadable Prepaid Card**: Contact the card issuer to report fraud and have the card number frozen.
- **MoneyGram**: Contact MoneyGram ASAP to stop the money transfer.
- **Western Union**: Contact Western Union's Fraud Hotline ASAP to stop the money transfer.
- **Bank Wire Transfer**: Contact the bank ASAP to have the wire recalled.

For funds that were not sent recently:

- **U.S. Mail:** Email the address and tracking number to General Analyst Sharon Miller. The provided address will be flagged and hopefully other victims will be helped through the information provided.
- **Reloadable Prepaid Card, MoneyGram, and Western Union**: Report the fraudulent transaction to the company so that the data will be recorded in the company's databases.
- **Bank**: Report fraudulent transactions to the bank. Close the bank account and open a new one, as scammers may attempt o use the account number or pass it on to other criminals.
- **File a complaint with the FTC.**

Additional Steps to Assist in Recovery

- Report the victimization to local police, federal law enforcement, and the Federal Trade Commission.
- Change the cellular or landline telephone number of the victim
- Forward mail to a PO Box or to a family member. This will eliminate a lot of the standard mail (which is the type that scammers usually use to solicit victims). This may not eliminate all the fraudulent mailings, unfortunately.
- Close compromised bank accounts and credit cards. Set up online banking and allow a trusted family member to have access to monitor the financial transactions.
- Consider giving the older adult access to a small account for their normal bills and cash. Consider restricting that person's access to investment and savings accounts.
- Notify financial advisors and other banking personnel to be on the look out for large withdrawal requests.
- Obtain a free, yearly credit report from www.annualcreditreport.com or through calling 877/322.8228. A person can obtain one free annual credit report per year.
- Last resort: guardianship for the victim.



Knowledge is power! Please share this information with others who you believe would benefit from knowing it!