

Mass Marketing Fraud

What Is Mass-Marketing Fraud?

The term "mass-marketing fraud" refers generally to any fraud scheme that uses one or more mass-communication methods – such as the Internet, telephones, the mail, or in-person meetings – to fraudulently solicit or transact with numerous prospective victims or to transfer fraud proceeds to financial institutions or others connected with the scheme. Mass-marketing fraud schemes generally fall into two broad categories: (1) schemes that defraud numerous victims out of comparatively small amounts, such as several hundred dollars, per victim; and (2) schemes that defraud comparatively less numerous victims out of large amounts, such as thousands or millions of dollars per victim.

Law enforcement and consumer protection authorities sometimes classify particular fraud schemes by the communication mechanism used (e.g., "Internet fraud," "mail fraud," and "telemarketing fraud"). At the same time, they also recognize that mass-marketing fraud schemes often use multiple communication techniques to reach more prospective victims. For example, an advance-fee fraud scheme (further described below) may use a high volume of unsolicited emails ("spam") to make initial contact, encourage interested recipients to call a particular telephone number for further information, and mail materials to the potential victim, such as counterfeit checks. Mass-marketing fraud schemes can appear as "too good to be true" payments for goods or services required in advance, requests for personal information over the telephone, unsolicited offers, or high-pressure sales tactics claiming that immediate action is required to avoid losing a "once in a lifetime" opportunity.¹

What Are The Major Types of Mass-Marketing Fraud?

Advance-Fee Fraud Schemes

These schemes are based on the concept that a victim will be promised a substantial benefit – such as a million-dollar prize, lottery winnings, a substantial inheritance, or some other item of value – but must pay in advance some purported fee or series of fees before the victim can receive that benefit.

Online-Auction and Online-Retail Schemes

- Purport to offer high-value items - ranging from high-priced watches to computers to collectibles - that are likely to attract many consumers
- Induce victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods)
- Fraudsters might email prospective victims to say that they have additional quantities of the items that had been up for auction, but persuade them to visit other websites that do not offer the consumer protections found on legitimate auction sites

Business Opportunity or 'Work-at-Home' Schemes

- Contact people to advertise purported business opportunities that supposedly allow individuals to earn thousands of dollars a month in "work-at-home" ventures
- Typically require the individuals to pay hundreds of dollars (or more), but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business

Charity Schemes

- Solicit donations in the name of non-existent or fraudulent charities
- Mostly occur during the holidays or in the aftermath of disasters, when philanthropy is most common and potential victims are most vulnerable to giving money

Credit-Card Interest Reduction Schemes

- Contact individuals and offer to help them lower their credit-card interest rates, but charge fees without effecting actual reductions in the cardholders' interest rates

Inheritance Schemes

- Contact prospective victims representing that the people contacted are in a position to receive a substantial inheritance from a family member or from an individual who has died without heirs
- The victim is then subjected to a series of demands for advance payment of various nonexistent fees before the inheritance can be transferred

Foreign Lottery/Prize/Sweepstakes Schemes

- Falsely represent that the victim just won a substantial lottery prize or other sweepstakes or prize contest, but must pay what proves to be a growing number of nonexistent "fees" or "taxes"

before he or she can receive the prize

- Operate from a growing number of countries, such as Costa Rica, the Dominican Republic, Jamaica, the Netherlands, Nigeria, and Spain

Online Sales/Counterfeit Cashier's Check/Overpayment Schemes

- Operate by contacting people who use Websites to advertise large items they are selling, such as cars. The people who contact the prospective seller represent that they want to buy the item, but then send the seller a check for more than the purchase price
- The fraudulent "buyer" instructs the seller to use a money-transfer business to wire the funds in excess of the purchase price to the "buyer." Invariably, after depositing the check into his account, the seller soon finds that the check is counterfeit
- The seller not only loses the funds wired to the "buyer," but may also incur liability as a result of depositing the counterfeit check

'Romance' Schemes

- Send out mass-emails in which the sender pretends to be a man or woman interested in a romantic relationship
- Victims who respond to such emails may be subjected to a lengthy stream of emails or even phone calls professing love and affection.
- Eventually, the victims may be persuaded to send substantial amounts of money to their "true loves," who lie about needing money to travel or to meet other unexpected expenses
- In some cases, victims are even talked into performing tasks that

directly further the scheme, such as receiving and redistributing counterfeit checks to be sent to other victims or receiving funds from other victims

Bank and Financial Account Schemes

Some mass-marketing fraud schemes involve tricking potential victims into providing their bank or financial account data, so that participants in the scheme can gain unauthorized access to those accounts and siphon off funds or charge goods to the victims' accounts. These types of schemes may also involve identity theft.

'Phishing'

- The use of emails and websites that falsely purport to be associated with legitimate banks, financial institutions, or companies, but that manipulate Internet users into disclosing personal and financial data

'Vishing'

- The telephone equivalent of phishing. Fraudsters often call prospective victims, pretending to be officials with the victim's bank and seek to trick the person into disclosing banking details during the call

Investment Opportunity Schemes

'Pump-and-Dump'

- Typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly-traded stocks or stocks of shell companies (the "pump"), then immediately sell-off their stock holdings (the "dump") to realize substantial profits before the stock price falls back to its usual low level. Stock buyers who are unaware of the false information become victims of the scheme once the price falls.


Short-Selling ('Scalping') Schemes

- Disseminate false or fraudulent information in an effort to cause price decreases in a particular company's stock in order benefit from short selling a stock. When a party short sells a stock and covers the trade by buying back the stock at a lower price, the party makes a profit on the difference between the higher price at which it was sold and the lower price at which it was bought back.

Other investment schemes involve direct solicitation of prospective investors through "cold calls" (i.e., calls to people whom the fraud scheme has not previously contacted) or email or phone contact lists of people previously contacted by members of fraud schemes. These include schemes that simply fail to invest the investors' money as promised, as well as "Ponzi" schemes (i.e., schemes that recruit multiple would-be investors, but use a portion of the funds received from later investors to pay to earlier investors to enhance the appearance of the scheme's legitimacy).

How Do I Protect Myself?

To reduce the risk of becoming a victim of Mass-Marketing Fraud, there are some basic steps you can take.

- Remove your name from solicitation lists. You may opt out of direct mail and email offers at www.dmachoice.org, credit card offers at www.optoutprescreen.com or (888) 567-8688 , and online cookie collecting at www.networkadvertising.org.
- Shred suspicious mail and do not respond to junk mail or emails from strangers.
- Do not participate in or respond to claims that you have won a foreign lottery, particularly any lottery or sweepstakes that you do not remember entering. Participating in a foreign lottery is against the law.
- Get all offers in writing and independently verify credentials.
- Don't deposit checks sent by companies that claim the check is for fees or taxes on lottery winnings or an inheritance from a long-lost relative. Before the bank discovers the check is counterfeit, the fraudster will request that you return a portion of the money via wire transfer.

What Can I Do If I Have Become A Victim of Mass-Marketing Fraud?

Report Fraud to Law Enforcement

- **Local Law Enforcement** – Contact your local law enforcement office to file a police report.
- **District Attorney** – Contact your local District Attorney's Office.

- **State Attorney General** – Contact your state's Attorney General's Office to report the fraud. Find contact information at www.naag.org.
- **Federal Law Enforcement** – Contact your local FBI Field Office or submit an online tip at <http://tips.fbi.gov>. Look up your local field office at www.fbi.gov/contact-us/field.

Report Fraud to the [Federal Trade Commission](https://www.ftc.gov)

- Lodging a complaint with the FTC will also enter the fraud into the [Consumer Sentinel Network](https://www.consumer.gov/sentinel) so that law enforcement can stop fraud. Please note that this process will not initiate a criminal investigation of your case.

¹[FBI Mass Marketing Fraud—Awareness & Prevention Tips](https://www.justice.gov/criminal-fraud/mass-marketing-fraud)