MSPA AMERICAS

# Internet Scam Response Guide

## I. How to Identify the Signs of a Scam

The Federal Trade Commission ("FTC") recommends that a business train its staff members to be on the lookout for internet scams. Signs that your business could be the target of a scam include:

- You receive a disproportionately large number of returned emails. This is a sign your email address and/or website might have been illegitimately copied and is being used to scam others.
    - Retain a copy of these emails and forward them to the FTC at spam@uce.gov

- You receive an email that was sent to a large number of recipients, but appears to be sent to you personally.

The Federal Bureau of Investigation ("FBI") and FTC recommend that companies become better educated about scams and protective measures by:

- Visiting their Scam Alert websites:
  http://www.consumer.ftc.gov/scam-alerts
  Note that mystery shopping is explicitly listed on this website.

  http://www.ic3.gov/about/default.aspx

  Joining the FTC's Scam Alert email list:

  https://public.govdelivery.com/accounts/USFTC/subscriber/new?topic_id=USFTC_31.

## II. Respond Promptly in the Event You have Been Targeted by a Scam

State and Federal law enforcement officials are prepared to respond to internet scams. The FBI and FTC recommend the following actions in response to internet scams:

- Create a file of evidence of the scam. The more information you can collect regarding a scam and provide to law enforcement officials, the more likely they will be able to shut down the perpetrator. The following are examples of relevant information:[1]

    - Any contact information of the individual or business that perpetrated the scam:
        - E.g., any name, address, telephone number, email address, and/or website.
        - The name and position of any representatives.

[1] Federal Bureau of Investigation – Internet Crime Complaint Center, Frequently Asked Questions, available at http://www.ic3.gov/faq/default.aspx.

- Specific details of the scam:
  - Dates of any events or transactions;
  - The dollar amount of any loss;
  - Method of payment; and/or
  - Method of contact
- Pertinent documents regarding the scam:
  - Printed or electronic copies of emails;
  - Printed or electronic copies of webpages;
  - Documentation of payment;
  - Envelopes from mail correspondence;
  - Chat room or text message transcripts; and/or
  - Facsimiles
- Contact information for potential witnesses.
- Contact information for other victims.

- Report fraudulent or suspicious emails and websites to your internet service provider. It can investigate and potentially shut down the perpetrator.[2]

- If you believe your website has been spoofed, notify your webhosting service. It can assist you with any additional remedial steps and help investigate the incident.[3]

- Report incidents to law enforcement officials:[4]
  - File a report with the FTC. The information in your report will assist FTC and other law enforcement agencies in investigating the incident. https://www.ftccomplaintassistant.gov/Information#crnt&panel1-1

  - Report incidents to your State's Attorney General.

    - A listing of State Attorney Generals can be found here: http://www.naag.org/current-attorneys-general.php

  - File a report with the FBI's Internet Crime Complaint Center if you were the victim, were targeted, or are aware of a scam. http://www.ic3.gov/complaint/default.aspx

  - Report scams perpetrated though the mail to your local postmaster.

If all member companies are vigilant in becoming educated about internet scams and in promptly reporting suspicious internet activity, the mystery shopping industry will become an increasing unattractive target for scammers.

---

[2] Federal Bureau of Investigation, *FBI Says Web "Spoofing" Scams are a Growing Problem*, available at http://www.fbi.gov/news/pressrel/press-releases/fbi-says-web-spoofing-scams-are-a-growing-problem/.

[3] *Id.*

[4] Federal Trade Commission, 10 Ways to Avoid Fraud, available at http://www.consumer.ftc.gov/articles/0060-10-ways-avoid-fraud; Federal Bureau of Investigation, *FBI Says Web "Spoofing" Scams are a Growing Problem*, available at http://www.fbi.gov/news/pressrel/press-releases/fbi-says-web-spoofing-scams-are-a-growing-problem.