CONTACT:
Research Section
5000 NASA Blvd.
Suite 2400
Fairmont, WV 26554
Ph: 304-367-1994
Fax: 304-366-9095
Web: www.nw3c.org

Telemarketing Fraud (June 2017)

The effectiveness of telemarketing fraud stems from the use of telemarketing (contact made by phone, email, internet) to conduct business by many reputable companies. Fraudsters depend on the proliferation of legitimate telemarketing to help deceive the potential victim into revealing valuable personally identifiable information. Telemarketing fraud often involves some sort of victim compliance whether it involves the victim initiating contact with the perpetrator or voluntarily providing their private information to the offender; thus, fraud victims may experience feelings of shame and embarrassment that may prevent them from reporting victimization.

According to research conducted in several statewide surveys, around the country, fraudulent telemarketing techniques have victimized 26% of the entire U.S. adult population at some point in their lives.[1]

Definition

Telemarketing fraud refers to any type of scheme in which a criminal communicates with the potential victim via the telephone.[2] The difficulty with accurately defining telemarketing fraud is that the telemarketing aspect of an illicit act can precede fairly wide variety of fraudulent activities. The consumer Sentinel Network 2016 report indicates that the telephone is still the tool of choice for fraudsters to use when looking for victims, comprising 77% of all complaints to the Federal Trade Commission (FTC).[3] Despite the ubiquity of personal computers in today's society, the three year trend indicates that the use of the telephone to commit fraud has actually increased by 23%, from 385,823 to 543,088, since the 2014 year-end report, and the use of the email, internet and web sites coming in a distant second and third at 8% and 6% respectively.[4]

How It Happens

Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services. Telemarketing can also serve as a method for unscrupulous individuals to obtain the Personally Identifiable Information (PII) from a victim, needed to commit identity theft. A wide variety of fraud types are perpetrated via telemarketing. Telemarketing itself is actually legal as long as the product or service being marketed is legitimate, and it can be an effective method for reaching prospective customers. The fraudulent aspect of telemarketing fraud transpires when the product or service being sold is not delivered as described or is totally absent.

Scammers use exaggerated — or even fake — prizes, products or services as bait. Some may call you, but others will use email, texts, or ads to get you to call them for more details. Some typical examples of telemarketing scams include the following. (**Note**: the following is by no means intended to represent a complete listing of the potential types of telemarketing fraud; rather, it is intended to illustrate the wide range of activities that can fit the category.)

- **Tech Support Scam:** Unsolicited calls allegedly from representatives of Microsoft or some other software company that claim the anti-virus software on the victim's computer needs to be updated due to a newly discovered threat. The end goal is to convince the victim to turn over control of their computer to the caller to supposedly update the anti-virus software, fix a registry error or some other defect. The victim is informed that the vital service will cost usually several hundred dollars. The victim provides credit card information that is charged for the fake service, the contents of the victim's computer is compromised and their PII is obtained which can be used to perform even more damaging identity theft.
- **Credit and Loans:** Advance fee loans, payday loans, credit card protection, and offers to lower your credit card interest rates are very popular schemes, especially during a down economy. A variation of this type of scam involves offers to help alleviate high interest student loans. After the victim provides PII, a fee is solicited for the service being offered, periodic payments to the caller's company are sometimes arranged, none of which are used for loan relief efforts.
- **Sham or Exaggerated Business and Investment Opportunities:** Scammers rely on the fact that business and investing can be complicated, and that most people don't research the investment. Business opportunities are described that sound foolproof and are 'guaranteed' to make the victim financially secure. In order to take advantage of these opportunities the victim simply provides PII and an up-front fee.
- **Charitable Causes:** Urgent requests for recent disaster relief efforts are especially common on the phone. Any time a high profile incident takes place that makes the news, whether it's a weather related disaster or some incident resulting in mass casualties, these types of calls begin to appear.
- **High-Stakes Foreign Lotteries:** These pitches are against the law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. What's more, you may never see a ticket.
- **Extended Car/Home Warranties:** Scammers find out what kind of car you drive, or that you have recently purchased a new home and when you bought it so they can urge you to buy overpriced — or worthless — plans.
- **The "Yes" Scam:** A recent scam that involves a caller asking questions that sound legitimate, often pertaining to PII and credit card accounts. During the conversation, the caller asks a series of questions designed to get the victim to say the word "yes" or something sounding like an affirmative response, which is recorded and later used as justification for billing the victim for a service. When

the victim files a complaint, the caller uses the recorded affirmative comments to support their claims of legitimate transactions.

- **Debt Collection Scams:** According to a study performed by the American Association of Retired Persons (AARP), "phone calls from fake IRS agents have netted crooks about $47 million in three years, and the trend is expected to continue next year, but with a twist. The newest likely target will be people with college loans, who are threatened with arrest and other penalties unless a nonexistent "federal student tax" is immediately paid."[5]
- **The Grandparent Scam:** While there are multiple versions of this type of scam, it essentially involves a call to a grandparent or parent from someone claiming to be an associate of a family member (usually a high school or college age student) who happens to be visiting either another state, or a foreign country. The family member is reported to have been either arrested and needs bail money, or involved in some sort of accident resulting in hospitalization and in need of money. The victim is convinced to send money to the caller to assist their family member.
- **Credit Account Verification Calls:** Often 'robo' calls to the potential victim indicating that the call is in reference to the target's credit card account. The call states that there is nothing amiss with the account, but rather to advise the target of an opportunity to greatly reduce their interest rate. The victim must call back to provide PII and credit card numbers. The goal here is to gain access to the victim's accounts and potentially use their PII for identity theft.
- **Charity Scams:** The caller portrays a charity that might be popular at the time, whether a cancer related charity, veteran charity, or even stray animal charity. During the interaction the fake representative elicits enough PII and account information to remove funds from the victim's credit card, bank account or other sources of payment.

Costs and Statistics

It is difficult to determine the actual cost of telemarketing. Only a fraction of the telemarketing frauds and frauds in general are ever reported for a number of reasons, but probably the most prevalent reason is that the victim is too embarrassed to admit that they have been "had". There are many variations of the activity with more cropping up daily. Attributing a specific cost to the activity will never be accurate. The best that can be done is to obtain an estimate based on the reported incidents of such activities. According to a recent report from the Better Business Bureau, "Each year, millions of Americans fall prey to telemarketing fraud at a cost of $40 billion. Statistics indicate that about eight out of every ten elderly people are targeted by telemarketing scams."[6]

High Profile Examples/Case Studies

- In one of the biggest busts of its kind, the FTC charged four national cancer charities (the Cancer Fund of America, Cancer Support Services, the Children's Cancer Fund of America and the Breast Cancer Society) with defrauding

consumers of $187 million.[7] Defendants falsely portrayed themselves as legitimate charities with substantial programs that provided direct support to cancer patients throughout the United States, and falsely promised to provide patients with pain medication, transportation to chemotherapy, and hospice care, among other things. Defendants solicited contributions through direct mail, websites, and in phone calls such as this one, made on behalf of defendant Children's Cancer Fund. Instead of supporting patients battling the ravages of cancer, the overwhelming majority of donations benefitted the individual defendants, their families and friends, and the fundraisers hired to solicit contributions.[8]

- A California man has been sentenced to 16 years in federal prison for his part in what prosecutors believe is the largest mortgage modification scam in history, defrauding victims out of $31 million. According to prosecutors, the scammers would purchase lists of potential victims: homeowners at risk of foreclosure because they had fallen behind on mortgage payments. They would then email their targets, falsely claiming that the homeowner's mortgage was currently under review and that the mortgage lender had already considered and approved a modified rate for the loan. The scammers collected fees, did not turn them over to the banks, and did not provide legal representation. At best, the scammers did nothing more than fill in an application for a mortgage modification through the government's Home Affordable Modification Program (HAMP), a process that any homeowner can do on their own for free. In some cases, not even that minimal effort was exerted.[9]

- On March 18, U.S. District Judge J. Curtis Joyner issued a temporary order to halt the scam. Then, after a hearing on March 27, three defendants agreed to court-issued preliminary injunctions, and the court imposed a preliminary injunction against the final defendant, Ari Tietolman and his companies. Tietolman, the alleged leader of the telemarketing scheme, and his associates established a network of U.S. and Canadian entities to carry out their scam, according to a complaint filed by the Commission. The defendants used a telemarketing boiler room in Canada, where Tietolman lives, to cold-call seniors claiming to sell fraud protection, legal protection, and pharmaceutical benefit services. The cost for the defendants' alleged services ranged from $187 and $397. In some instances, the telemarketers who carried out the fraud impersonated government and bank officials, and enticed consumers to disclose their confidential bank account information to facilitate the fraud. The defendants used that account information to create checks drawn on the consumers' bank accounts. They then deposited these "remotely created checks" into corporate accounts established in the United States. The U.S. based defendants then transferred the money to accounts controlled by the Canadian defendants, according to an analysis of bank record. The FTC alleges that the defendants' conduct violated the FTC Act and the FTC's Telemarketing Sales Rule and that the telemarketing scheme drew in over $20 million dollars during only two years of operation.[10]

- A Missouri man has been added to an indictment that claims a nationwide telemarketing fraud targeting the elderly grossed $20 million, federal prosecutors.

Philip Hale, 36, of St. Louis was among a group of ten people added to nine people from the Phoenix, Ariz. area who were indicted in U.S. District Court in St. Louis in October 2016, prosecutors said. The group ran a fraudulent business opportunity scheme from telephone "boiler rooms" in Phoenix and grossed $20 million in sales from U.S. and Canadian residents, prosecutors said. They were claiming to offer merchants services to process credit card transactions, but were not in the merchant processing services business, the indictment says.[11]

The Response/Current Efforts

Legislation designed to reduce or eliminate unwanted contact by telemarketers, regardless of whether they are legitimate or not, is continually being pushed by advocacy groups and legislators. The most recent such action occurred on June 18, 2015 when the Federal Communications Commission (FCC) approved new rule modifications to the Telephone Consumer Protection Act (TCPA) that did not differentiate between telemarketing scammers and legitimate telemarketers. The new rules provide:

- Telephone service providers can offer robocall blocking technologies to consumers. Providers previously asserted the FCC prohibited such technology.

- Consumers now have the right to revoke their consent to receive calls and text messages sent from autodialers in any reasonable way at any time.

- To prevent "inheriting" consent for unwanted calls from a previous subscriber, callers will be required to stop calling reassigned wireless and wired telephone numbers after a single call.

- The TCPA prohibits the use of automatic telephone dialing systems to call wireless phones and to leave prerecorded telemarketing messages on landlines without consent. "Automatic telephone dialing system" is defined as "equipment which has the capacity to (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[12]

In 2016, the FCC began to toughen their stance on enforcement of the TCPA. According to one report, the 2015 modification to the TCPA rules were taken as 'more of a suggestion' however, going into 2016 enforcement is being stepped up signaling that the FCC intends to enforce the rules more rigidly.

- On Oct. 26, 2015, TD Bank was hit with a punitive class-action lawsuit in the New Jersey District Court, following allegations that the company violated TCPA regulations. According to Lexology, the lawsuit seeks to classify all individuals who received unsolicited phone calls to their mobile phones from TD Bank's automated dialing system. The case stemmed from an incident where a customer claimed TD Bank called his cell phone about a debt using either a prerecorded or artificial voice, despite the customer having denied his consent to do so.[13]

O August 11, 2016 further toughened their stance when they adopted an order, FCC 16-99 that is intended to;

- Implement Section 301 of the Bipartisan Budget Act of 2015, which amends the TCPA by excepting from that Act's consent, the requirement that robocalls "made solely to collect a debt owed to or guaranteed by the United States" and authorizing the Commission to adopt rules to "restrict or limit the number and duration" of any wireless calls "to collect a debt owed to or guaranteed by the United States." The Budget Act requires the Commission to "prescribe regulations to implement the amendments made" by Section 301 within nine months of enactment. In implementing these provisions, we recognize and seek to balance the importance of collecting debt owed to the United States and the consumer protections inherent in the TCPA.[14]

What to do:

In order to reduce the number of telemarketing calls receive, NW3C suggest these tactics:

- Sign up for the National Do Not Call Registry. The Registry is maintained by the FTC. If a telemarketer contacts you after you've added yourself to the list, you can file a complaint with the FTC.
- When possible, minimize the amount of personal data that you share with the government and businesses. For instance, if a retail store requests your phone number, do not share it with the store unless it is necessary to complete a transaction. Additionally, do not place your phone number on product surveys or warranty cards. Surveys and warranty cards are used to profile and target individuals for more advertising.
- Opt-out of telemarketing, credit reporting agency, and Customer Proprietary Network Information (CPNI) databases. The CPNI data base is collected by the telecommunications company that the user subscribes to for their phone service. It consists of time, date, duration and destination of the call among other information. Most companies allow for opt-out, but that fact is usually buried deep within the user agreements.
- Under the law, you have the legal right to request the "telemarketer's do not call policy." Consider asking telemarketers who call you to send the list to you by certified mail. If they fail to do so, you may have a right of action against them for $500 minimum damages.
- File a complaint with the Federal Communications Commission (FCC) if you believe that you are the victim of illegal telemarketing. (see information links below for URL)
- Notify your attorney general if you believe that you are the victim of illegal telemarketing.
- For a listing of all attorney generals, see the National Association of Attorneys General Website.

“For More Information” Links

FTC’s online complaint assistant located at; https://www.ftccomplaintassistant.gov/#&panel1-1 or call 1-877-FTC-HELP (1-877-382-4357).

Internet Crime Complaint Center (IC3) located at; www.ic3.gov

Federal Bureau of Investigation, (FBI) located at www.FBI.gov

Better Business Bureau, located at; www.bbb.org

The Electronic Privacy Information Center, located at; https://epic.org

The National Fraud Information Center, located at; http://www.fraud.org/homepage

The Federal Trade Commission’s ‘Do Not Call Registry’ web site, located at; https://www.donotcall.gov/

National Association of Attorney’s General, located at; http://www.naag.org/

Maintenance and revisions: NW3C Research Department

Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Smart Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Endnotes

[1] Fraud Statistics, provided by the Retirement Industry Trust Association Senior Fraud Initiative, located at; http://www.ritaus.org/fraud-statistics

[2] Phone and Telemarketing Fraud, definition, retrieved from the internet on June 2, 2017,located at; https://www.law.cornell.edu/wex/phone_and_telemarketing_fraud

[3] Consumer Sentinel 2016 Data book of complaints filed, located at; https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

[4] Ibid. CSN, p. 9

[5] Scams to Watch for in 2017 by Sam Kirchner, published by AARP, located at; http://www.aarp.org/money/scams-fraud/info-2016/2017-scams-to-avoid.html

[6] Warning: Avoid Becoming a Telemarketing Fraud Victim, by John North, President Dayton, OH. Better Business Bureau, published in Dayton Daily News, March 22, 2017, located at; http://www.mydaytondailynews.com/business/warning-avoid-becoming-telemarketing-fraud-victim/hyE9s14sC7E6KjtVBmlmVL/

[7] A New Breed of Con Artists, by Joe Kita, published February 2016, in AARP Bulletin, located at; http://www.aarp.org/money/scams-fraud/info-2015/scams-and-frauds-to-avoid.html

[8] Opening Statement from Scham Cancer Charities Press Conference, by Jessica Rich, FTC. May 15, 2015, located at; https://www.ftc.gov/public-statements/2015/05/opening-statement-sham-cancer-charities-press-conference

[9] Man Behind $31 Million Dollar Mortgage Telemarketing Scam Sentenced to 16 Years in Prison, by Chris Moran, published 9/16/2016, in the Consumerist, located at; https://consumerist.com/2016/09/16/man-behind-31-million-mortgage-telemarketing-scam-sentenced-to-16-years-in-prison/

[10] FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out Of Millions, FTC Press Release March 2014, located at; https://www.ftc.gov/news-events/press-releases/2014/03/ftc-stops-mass-telemarketing-scam-defrauded-us-seniors-others-out

[11] Missouri Man Added to Nationwide Telemarketing Fraud Case, by Robert Patrick published in the St. Louis Post Dispatch, March 13, 2017, located at; http://www.stltoday.com/news/local/crime-and-courts/missouri-man-added-to-nationwide-telemarketing-fraud-case/article_97ba857c-18e5-5d85-bb5f-a3e65d5a87e6.html

[12] FCC Approves New TCPA Rules - Telephone Consumer Protection Act, Published in the national Law Review, Thursday, June 18, 2015 located at; http://www.natlawreview.com/article/fcc-approves-new-tcpa-rules-telephone-consumer-protection-act

[13] Why You Need To Pay close Attention to TCPA in 2016, published on the Connect First blog, located at; http://blog.connectfirst.com/blog/security-compliance/need-pay-close-attention-tcpa-2016

[14] Federal Communications Commission order FCC 16-99, adopted August 2, 2016 released August 11, 2016, CG Docket N0. 02-278 located at; https://www.fcc.gov/general/telemarketing-and-robocalls