

# Taking Action

## An Advocate's Guide to Assisting Victims of Financial Fraud

REVISED 2018



THE NATIONAL CENTER FOR  
**Victims of Crime**

SaveAndInvest.org

**FINra**  
Investor Education  
FOUNDATION

# Helping Financial Fraud Victims

June 2018

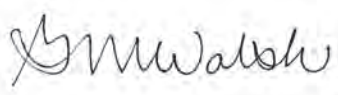
Financial fraud is real and can be devastating. Fortunately, in every community there are individuals in a position to provide tangible help to victims. To assist them, the Financial Industry Regulatory Authority (FINRA) Investor Education Foundation and the National Center for Victims of Crime joined forces in 2013 to develop *Taking Action: An Advocate's Guide to Assisting Victims of Financial Fraud*.

Prevention is an important part of combating financial fraud. We also know that financial fraud occurs in spite of preventive methods. When fraud occurs, victims are left to cope with the aftermath of compromised identities, damaged credit, and financial loss, and a painful range of emotions including anger, fear, and frustration.

This guide gives victim advocates a roadmap for how to respond in the wake of a financial crime, from determining the type of fraud to reporting it to the proper authorities. The guide also includes case management tools for advocates, starting with setting reasonable expectations of recovery and managing the emotional fallout of financial fraud. Initially published in 2013, the guide was recently updated to include new tips and resources.

Our hope is that this guide will empower victim advocates, law enforcement, regulators, and a wide range of community professionals to capably assist financial victims with rebuilding their lives.

Sincerely,



Gerri Walsh  
President  
FINRA Investor Education Foundation



Mai Fernandez  
Executive Director  
National Center for Victims of Crime

# About Us

The **Financial Industry Regulatory Authority** (FINRA) is a not-for-profit self-regulatory organization authorized by federal law to help protect investors and ensure the fair and honest operation of financial markets. Under the supervision of the Securities and Exchange Commission (SEC), we regulate the activities of U.S. broker-dealers and perform market regulation pursuant to our own statutory responsibility and under contract for certain exchanges.

Through the **FINRA Investor Education Foundation**, we provide investors with high-quality, easily accessible information and tools to better understand the markets and the basic principles of saving and investing. The FINRA Investor Education Foundation's investor protection campaign seeks to protect investors from investment fraud by helping them:

- recognize they are vulnerable to financial fraud;
- identify persuasion techniques; and
- reduce risky behaviors by asking questions and checking information.

Through tools and resources, available at the [SaveAndInvest.org](https://www.saveandinvest.org) website, the FINRA Foundation helps you teach consumers to make informed financial decisions—and arms you with the information you need to protect others from investment fraud.

---

The **National Center for Victims of Crime** is the nation's leading resource and advocacy organization dedicated to serving individuals, families, and communities harmed by crime. The mission of the National Center is to forge a national commitment to help victims of crime rebuild their lives. Working with local, state, and federal partners, the National Center:

- provides direct services and resources to victims of crime throughout the country;
- advocates for laws and public policies that secure rights, resources, and protections for crime victims;
- delivers training and technical assistance to victim service organizations, counselors, attorneys, criminal justice agencies, and allied professionals serving victims of crime; and
- fosters cutting-edge thinking about the impact of crime and the ways in which each of us can help victims rebuild their lives.

For more information, please contact:

National Center for Victims of Crime  
2000 M Street, NW, Suite 480  
Washington, DC 20036  
(202) 467-8700, [www.VictimsofCrime.org](https://www.VictimsofCrime.org)

# Acknowledgements

This guide would not have been possible without the effort and expertise of many individuals and organizations.

The National Center and FINRA Foundation would like to recognize the following organizations whose expertise assisted us in developing this guide. While listed below, their inclusion does not imply an endorsement of this guide.

.....

AARP

National Sheriffs' Association

California Elder Justice Coalition

Network for Victim Recovery of DC

Council of Better Business Bureaus, Inc.

The New York County District Attorney's Office

Executive Office for United States Attorneys

Office for Victims of Crime,  
U.S. Department of Justice

Federal Bureau of Investigation

U.S. Commodity Futures Trading Commission

National Adult Protective Services  
Association

U.S. Federal Trade Commission

National Association of Attorneys General

U.S. Postal Inspection Service

National Crime Prevention Council

U.S. Securities and Exchange Commission

National Identity Theft Victims Assistance  
Network

# Contents

## SECTION

### 1

#### Laying the Foundation

- 1 How to Use This Guide
- 2 Financial Fraud: Explained
- 6 Major Categories of Financial Fraud
- 12 Victims and Perpetrators of Financial Fraud
- 15 Costs of Financial Fraud

## SECTION

### 2

#### The Advocate's Role

- 19 A Victim-Centered Approach
- 21 Identifying Fraud Types
- 22 Setting Expectations
- 24 Networking

## SECTION

### 3

#### Action Steps by Fraud Type

- 29 Action Steps for Advocates
- 31 Identity Theft Action Steps
- 37 Investment Fraud Action Steps
- 41 Mortgage and Lending Fraud Action Steps
- 45 Mass Marketing and Other Fraud Action Steps

## SECTION

### 4

#### Prevention for Victims

- 51 Identity Theft Prevention Tips
- 52 Investment Fraud Prevention Tips
- 53 Mortgage and Lending Fraud Prevention Tips
- 53 Mass Marketing and Other Fraud Prevention Tips

## SECTION

### 5

#### Resources by Fraud Type

- 57 General Fraud Reporting and Prevention Resources
- 58 Identity Theft Resources
- 58 Investment Fraud Resources
- 59 Mortgage and Lending Fraud Resources
- 59 Mass Marketing and Other Fraud Resources

# Section 1 Laying the Foundation



# How to Use This Guide

*Taking Action: An Advocate's Guide to Assisting Victims of Financial Fraud* is for anyone who finds themselves in a position to help victims of financial fraud.

Those new to financial fraud will want to start at the beginning. This section, **Laying the Foundation**, offers an introduction to financial fraud: the types of crimes being committed and profiles of who commit these crimes and their likely victims.

Once a financial fraud is suspected or verified, the next step is to assist in the recovery process. **The Advocate's Role** and **Action Steps by Fraud Type** provide victim advocates with clear steps to share with victims to assist in their recovery. These chapters walk through how to report financial exploitation and ways for victims to take control of their assets and strengthen their recovery.

Preventing revictimization is also a key role of victim advocates. The **Prevention** section covers steps victims can take to reduce the likelihood of future victimization.

Finally, the **Resources** section lists all resources contained in the guide, categorized by type of fraud.

---

## Talking Points for Advocates

Throughout this guide there is model language for communicating important themes to victims. The statements are not intended to be repeated verbatim but instead are reminders to the victim advocate to normalize the victim's experience to facilitate his or her recovery.

## Please Note

Due to the dynamic nature of websites, users of this guide should be aware that resources described may change or move locations at any time. Advocates are encouraged to archive any resources they find particularly useful.



# Financial Fraud: Explained

All fraud uses deception to enrich the fraudsters. In the case of financial fraud, deception and misrepresentation are used in conjunction with financial products, investments, or personal assets such as a house. While financial fraud encompasses a wide range of illegal behavior, our focus is on frauds that primarily target individuals: Ponzi schemes, mortgage fraud, advance-fee schemes, and credit card theft are all-too-common examples.

While the actual fraud varies, a similar set of tactics is used to separate victims from their money, including:

- gaining victims' trust and confidence;
- using false information to induce victims to invest in or purchase products that don't exist; or
- stealing identifying information.

## A Big Problem

---

Obtaining an accurate estimate of fraud prevalence has been hindered by a number of factors. Estimates vary, sometimes widely, due to inconsistent definitions of fraud, differences in the types of fraud examined and the populations studied, underreporting of fraud, and the method used to measure fraud, such as law enforcement records or surveys. Prevalence estimates need to be considered in this context.

Recent studies estimate that between 11 and 15 percent of the population are self-reported victims of financial fraud. A Federal Trade Commission report from 2013 estimated 25.6 million people were victims of one or more of the financial frauds included in the survey during 2011. And a 2012 survey by the FINRA Foundation found that more than 8 in 10 respondents were solicited to participate in a potentially fraudulent offer, with 11 percent of



all respondents losing a significant amount of money after engaging with an offer.

Regardless of the varying prevalence rates, these and other studies conclude that financial fraud is a significant and costly problem. The Financial Fraud Research Center—a joint project of the Stanford Center on Longevity and the FINRA Foundation—estimated the financial cost of consumer scams in the U.S. to be nearly \$50 billion per year.

These numbers are likely the tip of the iceberg. Experts in the field are well aware that financial fraud is largely underreported. Reporting one's victimization is complicated by feelings of shame and guilt, as well as other complex factors, such as:

- not knowing where to turn;
- feeling that reporting wouldn't make a difference;
- fear that reporting will lead to a loss of legal or financial control;
- threats and intimidation from the perpetrators;
- loss of esteem or prestige in a victim's social group;
- concern that reporting may culminate in a family member or friend being arrested

or sent to prison, which is particularly concerning if the individual is dependent on the exploiter; and

- lack of confidence in the ability of authorities to respond and assist.

One valuable contribution victim advocates can make to the cause of fighting financial fraud is to encourage victims to **report the crime**. Advocates can help victims overcome the stigma of being "taken" by a fraudster. They can sympathize with what has happened but also emphasize the value of taking action—including reporting the crime to the proper authorities.



## How Fraud Happens

---

We've all heard the timeless admonition: "If it sounds too good to be true, it probably is." But fraudsters make their living by making sure the deals they tout appear both good and true. The trick is figuring out when "good" becomes "too good." The common thread that binds different types of fraud is the psychology behind the pitch. Many successful con artists are clever, disciplined, and highly skilled at what they do. Whether they make their pitch over the Internet, by telephone, through the mail, or in person, these criminals tend to use the same tactics time after time.

They're masters of persuasion, tailoring their pitches to match the psychological profiles of their targets. They start by asking seemingly benign questions—about their target's

health, family, political views, hobbies, or prior employers. Once they know which buttons to push, they'll bombard their targets with a flurry of influence tactics, which can leave even the savviest person in a haze. These methods are used to commit fraud by both strangers as well as family members or other loved ones.

Ultimately, fraudsters ensnare their victims into making an emotional, not rational, decision. To learn more about the psychology of a scam, visit the FINRA Foundation's [www.SaveAndInvest.org](http://www.SaveAndInvest.org).

It is impossible to compile a list of all the schemes used by perpetrators because the fraudsters—who spend their "careers" developing schemes to defraud victims—are

continually creating new, inventive scams. Knowing the exact scam is not as important as understanding that fraudsters rely on persuasion tactics designed to take assets from victims. The FBI, AARP's Fraud Watch Network, and the Better Business Bureau (BBB) Scam Tracker, among others, have compiled lists of common schemes,

available online at [www.fbi.gov/scams-safety/fraud](http://www.fbi.gov/scams-safety/fraud), [www.aarp.org/fraudwatchnetwork](http://www.aarp.org/fraudwatchnetwork), and [www.bbb.org/scamtracker](http://www.bbb.org/scamtracker). Both AARP and BBB have developed scam-tracking maps to help consumers see what types of fraud are prevalent in their community and to make it easier to warn others.



## Financial Fraud Statistics

---

Research on consumer financial fraud is spread across a number of fields—including behavioral economics, psychology, marketing, law, finance, and criminology. In order to centralize research on financial fraud, the FINRA Foundation sponsors a *Consumer Financial Fraud eJournal* on the Social Science Research Network. Subscriptions are free: [www.ssrn.com/link/consumer-financial-fraud.html](http://www.ssrn.com/link/consumer-financial-fraud.html).

The Financial Fraud Research Center—a project of the Stanford Center on Longevity and the FINRA Foundation—also consolidates the latest research and news across a range of disciplines (from psychology to criminology to marketing and more). For more statistics and research briefs, visit [www.fraudresearchcenter.org](http://www.fraudresearchcenter.org).

In the fall of 2017, the Bureau of Justice Statistics, a division of the Department of Justice, fielded a financial fraud victimization supplement to the National Crime Victimization Survey (NCVS). The supplement yielded a large national sample from which to draw insights about the scope of the problem. The availability of accurate data on financial fraud victimization is a critical component in the fight against it. For access to all NCVS data and reports, visit [www.bjs.gov](http://www.bjs.gov).



You were very brave to report this crime. You're helping yourself and a lot of other people by speaking up. Thanks to you, the authorities can put out the word about this crime and potentially keep other people from being victimized.

# Major Categories of Financial Fraud

Although there are countless instances of financial fraud, the vast majority fall into four major categories. A brief description of each category is provided below, followed by some of the most common schemes employed by fraudsters in each major area. A list of key resources, most of them on the web, accompanies each fraud category, along with a brief explanation of what those resources offer. Additional information about financial fraud is available in the [Resources](#) section at the end of this guide. Specific information about reporting and recovery for each category is provided in Section 3 of this guide, [Action Steps by Fraud Type](#).

## 1. Identity Theft

---

**Identity theft is a crime that involves the illegal access and use of an individual's personal and/or financial information.** Identity theft can result in financial loss and seriously damage a victim's credit history, requiring substantial effort to repair. Identity theft often sets in motion, or makes a victim more vulnerable to, other types of financial fraud.

Identity theft may be committed against anyone whose personally identifiable information (name, Social Security number, credit card number, date of birth, etc.) is exposed. In an increasingly electronic world, we are all at risk.

### Common Schemes

- **Imposter scams:** pretending to be a trusted individual to convince victims to provide personal information and send money.
- **Credit card skimming:** stealing a victim's credit card information during a legitimate transaction (i.e., at a restaurant, gas station or ATM).
- **Phishing:** using spam email or the phone to pose as a legitimate organization to lure victims into revealing bank or brokerage account information, passwords or PINs, Social Security numbers, or other types of confidential information. Smishing occurs through text messages with the same objectives as phishing.
- **Hacking:** electronically breaking into personal computers, databases at financial institutions, and online retailers to steal personal information.

- **Data breaches:** incidents in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- **Stealing a wallet or purse:** using someone's driver's license, personal checks, or credit or debit cards directly.
- **Dumpster diving:** searching through trash to find personal information to steal.

## 2. Investment Fraud

---

**Investment fraud generally refers to a wide range of deceptive practices that scammers use to induce investors to make investing decisions.** These practices can include untrue or misleading information or fictitious opportunities. Investment fraud may involve stocks, bonds, notes, commodities, currency, or even real estate, and the scams can take many forms. Fraudsters can turn on a dime when it comes to developing new pitches or come-ons.

Research funded by the FINRA Investor Education Foundation shattered the stereotypes of investment fraud victims. Initial and follow-up research found typical victims to be:

- predominantly male;
- financially knowledgeable (victims scored higher on financial literacy tests than non-victims);
- college educated; and
- self-reliant when it comes to making decisions.

In addition, victims tended to have above-average income, and many older investors (ages 55 to 65) showed a willingness to engage in financially risky behaviors. These behaviors included not checking the registration status of investment professionals or products, being open to new investment information and attending free-meal investment seminars, and relying on investment tips from people they knew.

### Common Schemes

- **Pyramid scheme:** when fraudsters claim that they can turn a small investment into large profits within a short period of time. But in reality, participants make money by getting new participants into the program. The fraudsters behind these schemes typically go to great lengths to make their programs appear to be legitimate multi-level marketing schemes. Pyramid schemes eventually fall apart when it becomes impossible to recruit new participants, which can happen quickly.
- **Ponzi scheme:** a person known as a "hub" attracts money from new investors and uses it to pay so-called "returns" to earlier-stage investors, rather than investing or managing the money as promised. Like pyramid schemes, Ponzi schemes require a steady stream of incoming cash to stay afloat. But unlike pyramid schemes, investors in a Ponzi scheme typically do not have to recruit new investors to earn a share of the "profits." Ponzi schemes tend to collapse when the fraudster at the hub

can no longer attract new investors or when too many investors attempt to get their money out—for example, during turbulent economic times.

- **Market manipulation or “pump and dump” scam:** a fraudster deliberately buys shares of a very low-priced stock of a small, infrequently traded company and then spreads positive, usually false, information to build (or “pump”) interest in the stock. Believing they’re getting in early on a promising investment, unknowing investors create buying demand, resulting in a rapidly increasing stock price. The fraudster then sells (or “dumps”) his or her shares at the higher price and vanishes, leaving many people caught with worthless shares of stock when it becomes apparent there was no basis for the positive outlook for the promoted company.

- **Advance-fee scheme:** the fraudster offers to pay an enticingly high price for worthless stock in the investor’s portfolio. However, the investor must remit a “processing fee” in advance to pay for the service. The fraudster receives the payment from the investor but never purchases the stock, as intended. Advance-fee schemes often apply to many other common financial frauds, including beneficiary and lottery scams and the oft-mentioned “Nigerian 419” scam. Regardless of the hook, the format is the same—the consumer is tricked into handing over his or her own funds with the expectation of something of greater value, which never materializes.

### 3. Mortgage and Lending Fraud

---

**Traditional mortgage fraud includes situations in which homebuyers and/or lenders falsify information to obtain a home loan.** False information can include overvalued appraisals, guarantees of low interest rates, inflated income, and the fraudulent use of someone’s name without the knowledge of that individual. This fraudulent activity can also include loan modification, foreclosure prevention, and other lending fraud, for example, in which a consumer is promised a service related to a mortgage (whether new or refinanced) in exchange for an up-front fee. Unfortunately, many of these loan modification and foreclosure prevention fraudsters take the pre-paid money and disappear before providing any services to the victim.

These scams use a variety of simple tactics to identify their financially distressed victims. Some scammers locate distressed borrowers from published foreclosure notices or other publicly-available sources. Others rely on mass-marketing techniques such as flyers, radio, television and Internet advertising to lure in distressed borrowers. Still others deceptively suggest an affiliation with a government agency to quickly earn the trust of unwitting victims.

## Common Schemes

- **Appraisal fraud:** loan officer fraudulently overvalues an appraisal to make a sale.
- **Mortgage rescue and loan modification scam:** an advance-fee scam where homeowners are lured with promises to save them from foreclosure or lower their mortgage payments—in exchange for an advance or monthly fee. Sadly, many of these homeowners never get the relief they have been promised.
- **Reverse mortgage scam:** while they can be useful products and are not fraudulent per se, reverse mortgages have been associated with high fees and aggressive marketing as an easy way for retirees to finance lifestyles—or to pay for risky investments—that can jeopardize their financial futures. In some cases, a victim pays an advance fee to obtain a reverse mortgage that is never provided.
- **Loan origination scheme:** perpetrator originates a loan using false information (e.g., misrepresenting the buyer’s income or employment).

## 4. Mass Marketing and Other Fraud

---

**Mass marketing fraud is the use of false promises of cash prizes, services, goods, or good works in exchange for fees, donations, or purchases.** This crime may be committed through the mail, telephone, email, television ads or infomercials, or any other form of mass or individual communication.

This fraud is often defined by the form of communication used to conduct it. Mail and wire fraud occur when U.S. mail or a wiring service, respectively, are used to further a fraud scheme—whether it originated in person, through the mail, by telephone, or over the Internet. In many cases, these violations are associated with other areas of fraud. For instance, a Ponzi scheme investment opportunity may be marketed through U.S. mail with “investment” payments made through a wire service.

Most of the schemes described below are perpetrated through an advance-fee scenario; the targeted consumer is enticed to send money first in anticipation of a much greater reward, opportunity, or return that is never realized.



## Common Schemes

- **Fake check scams:** a cashier's check is sent by mail along with a letter that claims the consumer has won a lottery or is otherwise owed money (perhaps is the beneficiary of an estate of a relative they've never met). The consumer is asked to pay a "processing fee" or "taxes" on their windfall before the funds can be released to them. The cashier's check is provided purportedly as an advance to help them pay the fee or taxes. The scammer instructs the victim to deposit the check into a bank account, extract all or a portion of the proceeds in cash from the bank account, and then send a payment via a wire transfer to cover the fee or taxes. By the time the victim and the bank discover the cashier's check is counterfeit, the wire transfer has been claimed by the fraudster, robbing the victim of the amount of the transfer.
- **Foreign lottery schemes:** promises of winnings from a fraudulent foreign lottery with the requirement that the "winner" pay an advance fee to cover taxes, before the winnings can be released.
- **Home-repair scams:** door-to-door campaigns or telephone calls, where scammers offer services at discounts or explain that changes and repairs need to be made immediately. The scammers often lack business licenses, ask for a large portion of the money up front, and either never start or start but never finish the job. Targets for these scams are typically older adults or low-income families.
- **Mystery shopper scams:** "hiring" a victim to serve as a mystery shopper to evaluate stores or restaurants; victim is conned into paying an advance fee to apply and then receives no compensation.
- **"Nigerian" email or telephone schemes:** an offer received by mail, telephone, or email for the "opportunity" to share a percentage of millions of dollars that the scammer purports to be transferring out of Nigeria or other countries; victim is scammed out of an advance payment that was required before receiving his or her "share."
- **Romance scams:** begins with fake profiles on online dating sites created by stealing photos and text from real accounts or elsewhere. Scammers often claim to be in the military or working overseas to explain why they can't meet the target in person. Over a short period of time, the scammer builds a fake relationship with the target, exchanging photos and romantic messages, even talking on the phone or through a webcam. Just when the relationship seems to be getting serious, a health issue or family emergency arises, or the scammer wants to plan a visit. No matter the story, the request is the same: they need money. After the victim sends money, there's another request, and then another. Or the scammer stops communicating altogether.
- **Sweepstakes schemes:** offerings that inform consumers they have "won" a sweepstakes (that they have, in most cases, never entered); victim is conned into paying taxes or service fees but ultimately receives no prizes or benefits.

- **Tax collection scams:** most often perpetrated by phone and take two basic forms. In the first version, the IRS “agent” says the target owes back taxes and pressures the target into paying by prepaid debit card or wire transfer. The scammer threatens arrest and fines for noncompliance. In the other version, scammers claim they are issuing tax refunds and will ask for personal information under the guise of transferring a refund. This information can later be used for identity theft.
- **Tech support scams:** target receives a telephone call or a computer screen popup from someone claiming to be with tech support from a well-known software company. Often the scammer will create a sense of urgency—the computer is sending error messages, they’ve detected a virus, or your computer is about to crash and you’ll lose all your data! The target is told only a tech support employee can fix the problem, and then asked to allow access to his or her machine. Once access is granted, the scammer will claim the computer is infected with viruses and offer to fix the problem...for a fee. That may not be the end of the scam. If allowed remote access, scammers may also install onto the computer, scanning files in search of personal information, which scammers can use to commit identity theft.
- **Work-from-home and business opportunity scams:** for a “small fee,” the ad says, individuals can learn how to earn money working from home or buying into a franchise business opportunity. But once they pay the fee, they find out the promoter never had any work or business opportunity to offer. Many times, after the victims send in money, they receive a letter instructing them to convince other people to buy into the same “opportunity” or some other product. The only way to earn any money is if others pay in.

# Victims and Perpetrators

## Who Are Victims?

---

Anyone can be a victim of financial fraud. Research consistently shows that victims come from all education levels and socio-economic backgrounds. There is no single profile of a victim of financial fraud, and there is no level of intelligence that can prevent a person from being victimized. Everyone is at risk.

Even though anyone can be a victim, some types of financial fraud are more prevalent among particular groups of people. For instance, victims of investment fraud are most often male, financially literate, college educated, and approaching or in retirement. Lottery fraud victims are more typically single, older consumers and those who have lower levels of education and income. Victims of violent crime are more likely to have experienced identity theft in the years prior to the violent crime than others.

It is important for victim advocates to understand that victims of financial fraud have

not only been financially devastated but also emotionally deceived. They often feel isolated and blame themselves and their intellectual capacity for the fraud. Financial predators are skilled operators of scams. They possess a shrewd understanding of human behavior and how to manipulate people. In some cases, perpetrators of financial fraud may also be family members of victims, which can increase victims' emotional turmoil. Recognizing that everyone is vulnerable to fraud, and making this clear to the victim, helps remove the embarrassment that can be so devastating.



**You are not alone. Millions of people are defrauded every year. And you are a target only because you have money and assets to steal—not because of a failing on your part.**

## High-Target Populations

---

Some populations are more frequent targets of fraudsters because of their age, health, or life situation. Among those targeted are:

- senior adults, especially those who depend on family and friends for their care or those who have physical or mental impairments;
- individuals who are physically impaired;
- individuals who have cognitive issues or age-related mental incapacity (e.g., dementia, including Alzheimer's Disease);
- those who are grieving the loss of a loved one;

- victims of domestic violence;
- minorities;
- new and near-retirees; and
- previous victims of financial fraud.

Fraudsters target such populations for a variety of reasons. They may think these groups will more easily hand over control of their finances due to cognitive disability, emotional fragility, or simply a desperate need for a quick financial fix. They may also target them for one simple reason: they have money. This is the case with new and near-retirees who may be likely to have access to retirement savings or pensions, and may be open to suggestions for how to handle these funds. It is also the case for those who have recently come into a financial settlement or monetary windfall—such as an inheritance, lottery winning, or professional athletics contract.

Not every person who encounters a fraudster becomes a victim of financial fraud. The victim’s response to the fraud appeal can affect the outcome. Researchers are particularly interested in identifying behaviors that differentiate victims from non-victims in similarly targeted populations. According to an AARP Foundation National Fraud Victim Study, other factors predisposing people to financial fraud (excluding identity theft) include:

- a high level of interest in persuasion statements that are commonly made by fraudsters and sales people; and
- increased exposure to sales situations, such as attending free-meal financial seminars and opening and reading all mail.

These considerations are important for advocates to recognize in individuals to help them prevent further victimization.

## Who Are Perpetrators?

---

For victim advocates, understanding who may be a potential exploiter is every bit as important as knowing who may be commonly targeted. Depending on the type of crime, perpetrators may be perfect strangers whom victims have never met, or individuals whom the victims know and trust, such as relatives, caretakers, friends, or colleagues.

Fraudsters often target their victims through traditional offline social networks, such as community service groups, professional associations, or faith-based organizations. Scammers infiltrate groups of individuals connected through common interests, hobbies, lifestyles, professions, or faith to establish

strong bonds through face-to-face contact and sharing personal interests before launching their schemes.

Perpetrators may include:

- Family members, especially those caring for the victim or those in a position of control over the family member’s care
- Caretakers
- Trusted advisers, such as:
  - » Accountants
  - » Attorneys
  - » Investment professionals
  - » Bankers

- Members or leaders of a victim’s affinity groups, such as:
  - » Religious bodies
  - » Civic groups
  - » Cultural groups
  - » Political parties
  - » Book clubs
  - » Community groups
  - » Professional organizations
- Strangers

In general, most perpetrators of financial fraud (outside of identity theft) are individuals whom the victim trusts. That trust is the vehicle for financial fraud and often makes the fraud particularly devastating to the emotional stability and confidence of the victim.

“  
These perpetrators are manipulative and highly organized. They use tactics to gain your trust. But by working together—being proactive and organized—we can put a stop to their violations and help you recover.

# Costs of Financial Fraud

## Emotional Costs

---

Financial fraud can exact a heavy emotional toll on its victims, whose reactions to being victimized may resemble those of other crime victims, including victims of violent crime. Understanding such reactions is key to aiding the emotional recovery of financial fraud victims.

The FINRA Investor Education Foundation's research report, *Non-Traditional Costs of Financial Fraud*, examined the broader impact of financial fraud and found that nearly two-thirds of self-reported financial fraud victims experienced at least one non-financial cost of fraud to a serious degree—including severe stress, anxiety, difficulty sleeping, and depression.



You have been through an emotional and financial shock. Your money may or may not be recoverable. But we can work together to rebuild your life and help you move forward.

Fraud victims often suffer from:

- denial;
- fear;
- guilt;
- shame;
- isolation;
- anger;
- loss of sleep;
- loss of self-confidence;
- loss of trust in others; and
- depression or anxiety, or a combination of the two.

Financial fraud victims often feel as though they should have known better or done more to prevent the fraud. It is important for advocates to stress that the blame for the crime belongs to the perpetrator, not the victim.

## Monetary Costs

---

Financial fraud amounts to billions of dollars lost annually. For individual victims, the cost can be devastating. In addition to losing significant sources of income and equity, victims often must spend months sorting through a confusing series of reporting requirements and dealing with financial institutions simply to stop the fraud from continuing to occur.

After all that, financial recovery may be limited or impossible. Advocates can help manage the expectations of the victim in relation to financial recovery. Victims need to understand that although recovery of lost assets may not be possible, they can take back control of their lives and financial futures, and put an end to the trauma and stress of being victimized.

Individual victim losses may include:

- time and money spent clearing up financial and credit records;
- lifetime or retirement savings, benefits, or personal property;
- home or home equity;
- retirement income;
- ability to live independently; and
- employment.

Financial loss can vary significantly by the type of fraud. Romance scams, which occur when a perpetrator uses feigned romantic intentions towards a victim to gain their affection then commits fraud, often result in significant loss. The average victim of a romance scam loses over \$100,000. Conversely, tax scams (a type of imposter scam where the perpetrator pretends to be calling from a government agency to demand



**Financial fraud is a crime of opportunity, much like burglary. You are not to blame for the fraud. No one deserves to be a victim of fraud, and you are certainly not at fault for this crime. The perpetrator is responsible.**

money or personal information) are quite common, but few victims report monetary loss.

The *Non-Traditional Costs of Financial Fraud* report also found that, beyond psychological and emotional costs, nearly half of fraud victims reported incurring indirect financial costs associated with the fraud, such as late fees, legal fees, and bounced checks. Twenty-nine percent of respondents reported incurring more than \$1,000 in indirect costs, and 9 percent declared bankruptcy as a result of the fraud. An important insight from this research is that nearly half of victims blame themselves for the fraud—an indication of the far-reaching effects of financial fraud on the lives of its victims.

In short, the costs of financial fraud go well beyond the loss of money, and include emotional and mental health costs for victims. Advocates can help victims by supporting them emotionally and helping them understand that they are not to blame. Advocates should connect victims with mental health resources. Finally, advocates can give victims a process to follow to report the crime and, to the extent possible, recover losses.

# Section 2 The Advocate's Role





# A Victim-Centered Approach

Advocates have several important responsibilities in working with victims of financial fraud, but the most important is to use a victim-centered approach. This goal is accomplished by communicating with compassion, managing the expectations of the victims, and assessing any additional safety concerns that arise out of the financial fraud. Advocates also need to assist victims in preventing further victimization as well as strengthening the network of services for financial fraud victims where possible. Finally, advocates need to help victims be attentive to their own emotional and mental health as they recover.

Victim advocates should use the training and skills they've developed for communicating with victims. Active listening skills, coupled with a victim-centered, compassionate approach to all communication, will help achieve a more positive outcome for the victim.

For additional information on managing financial fraud victims' cases, visit:

- The Office for Victims of Crime, *Expanding Services to Reach Victims of Identity Theft and Financial Fraud*, at [www.ovc.gov/pubs/ID\\_theft/welcome.html](http://www.ovc.gov/pubs/ID_theft/welcome.html).

For additional training on working with victims, visit:

- The Office for Victims of Crime, *Victim Assistance Training Online*, at [www.ovcttac.gov/views/trainingmaterials/dsponline\\_VATonline.cfm](http://www.ovcttac.gov/views/trainingmaterials/dsponline_VATonline.cfm).

## Tips for Creating a Victim-Centered Approach

---

### Show compassion:

- From the beginning, victims need to know you care for and respect them.
- Acknowledge the trauma the victim is experiencing at the outset.
- Victims need to know they are not to blame for being victimized.
- Victims may benefit from understanding the powerful persuasion tactics that scammers use.
- Do not infantilize or be too familiar with the victim, particularly if a victim is older.

### Listen actively:

- Maintain eye contact.
- Use a friendly tone of voice.
- Paraphrase information given by the victim.
- Let the victim share the story once through, uninterrupted.
- Ask open-ended questions.
- Affirm the victim's experience.

### **Be sensitive to the victim's fears and safety concerns:**

- Build relationships with victims and let them know you are there to help.
- Victims may take time to fully grasp what has happened to them.
- Victims may fear the perpetrator if he or she is a family member.
- Victims may also be victims of other forms of abuse by the perpetrator.
- Victims may have difficulty trusting anyone, including the victim advocate and others attempting to help.

### **Understand why victims may return to you for help multiple times:**

- The fraud may be ongoing.
- They discovered a new facet of the fraud or have additional information to share.
- They need additional support accessing services.
- They may be economically dependent on the exploiter.

### **Protect and advocate:**

- If relevant, create a safety plan to prepare the victim for future contact with the perpetrator.
- Report the financial fraud to law enforcement authorities, when appropriate.
- Assess the victim's need for referral to other professionals, including:
  - » Adult Protective Services;
  - » legal aid or other civil attorneys;
  - » not-for-profit consumer credit counseling;
  - » mental health support; and
  - » medical care or evaluation, especially if there are concerns about a victim's physical or mental capacity.

# Identifying Fraud Types

One important step in communicating with victims is identifying the type of financial fraud that occurred. Many victims may already know, but in some cases the advocate may be the first person to speak with the victim about the fraud. Identifying the type and extent of the financial fraud may be challenging.

Even if victims are willing to talk about their experience, they may have difficulty telling their story coherently. They may jump from one time period or detail to another. It is important for victim advocates to first listen, then ask questions. When possible, let victims tell the whole story once through, uninterrupted, from their own perspective. Then the advocate can try to help victims piece together a chronological, fact-based account of the fraud.

Using the following simple, open-ended questions will help the victim speak about the crime they experienced.

- Can you tell me what happened to you?
- Can you tell me about the person or group of people who did this to you?
- How did this take place?
- What has been the impact on your life?

It is important to ask just enough questions to understand the fraud, generally, so that you can direct the victim to the best possible authorities and resources. It is not the role of the advocate to serve as a fraud investigator.

# Setting Expectations

It is extremely important that advocates help victims set realistic expectations associated with the aftermath of a financial fraud. Helping victims manage their expectations about their recovery is critical.

From the beginning, victims need to know that emotional trauma is a common reaction to financial fraud and recovery. Feelings of anger, helplessness, even despair—and conditions such as sleeplessness and loss of appetite—may require the help of mental health professionals.

Additionally, victims need to be aware that full financial recovery is rare because fraudsters often dispose of assets immediately after they acquire them. It is possible that some assets may be recovered, but these may be negligible. Even when a case results in an award of restitution, the victim may receive only a small amount relative to his or her total losses.

While many victims may look to advocates for assurances that their assets are recoverable, advocates should guard against providing false hope—even a response of “maybe”—which could lead to further trauma if the end result is loss.

Laying out the following points can help provide meaningful assistance to financial fraud victims.

## What Victims Need to Know

---

- 1 Recovery requires work.** Victims need to work with regulatory, criminal justice, or social service agencies to address their problems, pursue justice, and take an active role in their recovery.
- 2 Reporting matters.** Reporting any financial fraud, no matter how small, helps law enforcement, regulators, and government agencies put a stop to the fraud, prevent the victimization of more consumers, and pursue the criminals committing the fraud. Reporting is also recommended if the victim is looking for financial recovery.
- 3 Full financial recovery is difficult to achieve.** Even when criminal prosecution results in a restitution order, victims rarely obtain full recovery of their losses.
- 4 Civil legal action might be necessary to get money or property back—but will not always be a viable option.** Victims of financial fraud often cannot get their money back unless they file their own civil lawsuit against the fraudster. Civil lawsuits take time and can be costly. If successful, the court might order the perpetrator to return some or all of the assets lost to fraud. But even then, it can be difficult to

collect, especially if the money or assets have disappeared.

**5 Resources are available.** There are resources available for victims to assist in their financial recovery. Many, but not all, are listed in the back of this guide. In addition, the National Center and FINRA Investor Education Foundation have created a series of checklists written for victims to help combat the devastating effects of financial crime and to provide individuals with critical information and resources. The free checklists target the four major areas of financial fraud, including identity theft, investment fraud, mortgage and lending fraud, and mass marketing and other fraud. Checklists can be downloaded for free at [www.VictimsofCrime.org/taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists).

**6 Recovery is also about health.** Recovery is not only about finances, but it is also about the victim facing any emotional trauma caused by the crime and potentially seeking help to process feelings and restore mental health.

**7 Some agencies may not communicate with victims beyond the initial reporting.**

However, reporting is important. For instance, filing a Federal Trade Commission (FTC) affidavit does not cause a case to be opened and pursued, but the affidavit filed with the FTC will allow victims to assert certain victim rights with credit reporting companies. Further, reporting helps agencies share information with other consumer protection organizations that may be working on prevention and detecting fraud more broadly.



**TAKING ACTION:  
Victim Recovery CHECKLIST**

Help victims track their progress with fraud-specific checklists at:

> [www.VictimsofCrime.org/taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists)

# Networking

One key way to assist victims is to help them find local agencies and individuals who can support their efforts to recover. Advocates can enhance the recovery process from fraud and increase opportunities for prevention by networking with other agencies dealing with financial fraud issues. Victim advocates can raise awareness about financial fraud and promote a comprehensive response by creating or joining informal networks within their communities to combat fraud.

Many jurisdictions have multidisciplinary centers, such as Family Justice Centers, Elder Justice Centers, Financial Abuse Specialist Teams, and other coalitions that can save advocates and victims hours by cross-coordinating assistance and services to victims. Below are some initial steps to help connect with existing networks of agencies working on behalf of financial fraud victims.

## Making Advocacy Connections

---

### Initial Steps

#### 1 **Contact your state's Attorney General's Consumer Protection Office**

This office will be able to alert you to existing networks within your state. Find contact information from the National Association of Attorneys General at [www.naag.org](http://www.naag.org).

#### 2 **Contact your state's Crime Victim Coalition**

Crime victim coalitions often know of multiple local agencies and individuals working in the area of financial fraud. Reaching out to your local coalition and involving it in your case will help provide a connection point for many agencies, and may inform you about task forces you didn't know about. One example of a task force is the Financial Abuse Specialist Teams (FAST). A FAST focuses on complex financial abuse cases. It may comprise public agencies only or public-private partnerships, which include a multidisciplinary range of private practitioners. Learn more from the National Center on Elder Abuse at <https://ncea.acl.gov/whatwedo/practice/teams-fast.html>.

## Additional Contacts

You may find that the network in your state does not encompass your locality, or the network needs further improvements. You should consider contacting some of the organizations and individuals below to strengthen ties. Many of the local law enforcement and other agencies in your jurisdiction will have financial fraud specialists on their staff. Connecting with these individuals will not only improve your service delivery but will also give you direct access to up-to-date resources to help victims.

### **Area Agency on Aging**

The primary mission of the National Association of Area Agencies on Aging is to build the capacity of its members to help older persons and persons with disabilities live with dignity and choices in their homes and communities for as long as possible. Find your local Area Agency on Aging online at [www.n4a.org](http://www.n4a.org).

### **Adult Protective Services**

NAPSA provides Adult Protective Services (APS) programs with a forum for sharing information, solving problems, and improving the quality of services for victims of elder and vulnerable adult mistreatment. Its mission is to strengthen the capacity of APS at the national, state, and local levels, to effectively and efficiently recognize, report, and respond to the needs of elders and adults with disabilities who are the victims of abuse, neglect, or exploitation, and to prevent such abuse whenever possible. Find out more at [www.napsa-now.org](http://www.napsa-now.org).

### **Banking Regulators**

The Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the National Credit Union Administration provide various regulatory services for banks and credit unions. Read more about these regulators and their jurisdictions at [www.sec.gov/answers/bankreg.htm](http://www.sec.gov/answers/bankreg.htm).

### **Better Business Bureau (BBB)**

The Council of Better Business Bureaus is the network hub for BBBs in the United States and Canada. There are 110 independent BBBs across North America that serve accredited BBB businesses and consumers in their local communities. Find your local Better Business Bureau at [www.bbb.org](http://www.bbb.org).

### **Civil Attorneys**

Local civil attorneys who work with victims of crime can often advise victims and help them with financial recovery (when appropriate) by seeking justice in civil court. Find attorneys in your area by contacting the National Crime Victim Bar Association at (844) LAW-HELP or visit [www.victimbar.org](http://www.victimbar.org). Additionally, local legal aid offices may be able to provide assistance to victims. Find legal aid offices at [www.lsc.gov](http://www.lsc.gov).

### **Financial Services Industry Professionals**

Many banks and investment firms have victim service staff responsible for serving your area. Including these individuals in your action plans may enhance your knowledge of what services are available for financial fraud victims.



### **Investment, Securities, and Insurance Regulators**

Investment, securities, and insurance regulators are often willing to help prevent fraud and are important contacts for reporting. There are state, federal, and national regulators, many of which are included in the list of [Resources](#). Consider reaching out to the relevant FINRA District Office, [www.finra.org/industry/finra-district-offices](http://www.finra.org/industry/finra-district-offices), or SEC Regional Office, [www.sec.gov/contact/addresses.htm](http://www.sec.gov/contact/addresses.htm). Locate your state securities regulator at [www.nasaa.org](http://www.nasaa.org) and your state insurance regulator at [www.naic.org](http://www.naic.org).

### **Law Enforcement Officials**

Local and state law enforcement officials who investigate financial crimes are key information sources for victim advocates. Law enforcement is often willing and able to investigate these crimes, and your advocacy on behalf of victims may help those victims get the attention required. Law enforcement may also help you set realistic expectations for the victim concerning criminal prosecution.

### **Local Prosecuting Attorney**

Your state's prosecuting attorney will likely have at least one attorney who specializes in financial crime. Connecting with this individual or office will help you learn how these cases are prosecuted, set expectations, and advocate for the victims you serve.

### **Local Triad Program**

A Triad is a partnership of three types of organizations—law enforcement, older adult, and community groups—to promote older adult safety and reduce the fear of crime that older adults often experience. The National Association of Triads (NATI) provides grassroots-level assistance to help communities organize local Triads. It also provides a clearinghouse of programs and resources for local implementation, as well as training materials for law enforcement, volunteers, and community groups. Find out if there is a Triad in your area at [www.sheriffs.org/programs/national-triad](http://www.sheriffs.org/programs/national-triad).

# Section 3 **Action Steps** by Fraud Type



# Steps for Advocates

Regardless of the type of financial fraud a victim is experiencing, victim advocates should take the following action steps to help victims resolve the current fraud, protect themselves both now and in the future, and heal from the crime.

## STEP 1 – Refer Victims to Resources

---

Victim advocates play an important role in helping victims of financial fraud assess what happened and identify the most appropriate

resources for reporting and recovery. A list of resources is included at the end of this guide and referenced throughout.

## STEP 2 – Safety Planning

---

Safety planning may be necessary in some cases of financial fraud. In cases with co-occurring domestic violence, stalking, or elder abuse, the advocate should take care to ensure that the financial fraud safety plan includes a physical safety plan. Victim advocates can use their training in safety planning to assist victims with co-occurring safety concerns. For assistance in making physical safety plans, contact the Office for Victims of Crime Training and Technical Assistance Center at (866) OVC-TTAC. The suggestions below are designed as a starting point for financial safety planning, but are in no way exhaustive.

If the perpetrator is a family member or knows where the victim lives:

- have the victim think of a safe place to go if afraid of the perpetrator retaliating;

- have the victim make a list of safe people to contact for assistance; and
- consider calling Adult Protective Services, if necessary (see Step 3 below).

In general:

- encourage the victim to change his or her phone number if contacted by the perpetrator by phone;
- ask the victim to screen calls, and take calls only from those people whom the victim trusts;
- guide the victim to put his or her phone number on the Do Not Call Registry at [www.donotcall.gov](http://www.donotcall.gov) or by calling (888) 382-1222;
- save and document all contacts, messages, injuries, or other incidents involving the perpetrator; and

- follow the prevention steps located in Section 4 of this guide to protect against future fraud.

### **Step 3 – Assess the Need to Contact Adult Protective Services**

---

If the victim is an adult with impairments due to physical or mental disabilities, the advocate needs to assess if Adult Protective Services (APS) should be involved. This assessment is necessary whether the perpetrator is a family member or

a stranger, and referrals to APS should be made as appropriate. Use the National Adult Protective Services Association locator at [www.napsa-now.org](http://www.napsa-now.org) or call (202) 370-6292.

### **Step 4 – Refer to Mental Health Counselors**

---

Financial fraud can take a toll on the mental and emotional health of victims. Victim advocates should refer victims to local mental health counseling, as appropriate. Some victims may need financial assistance to see a mental health professional, so referrals to agencies that can provide low-cost mental health counseling are important.

# Identity Theft Action Steps

Recovery from identity theft requires victims to take many steps on their own behalf. Victims need to keep complete records to document what has happened. They need to file complaints with the appropriate agencies and know what to expect when they contact these agencies. The information below provides useful guidance for victims of identity theft.<sup>1</sup>

## STEP 1 – Place a Fraud Alert

The victim should first place a fraud alert with one of the three credit reporting companies in order to be notified of any fraudulent requests for credit. The victim will need to:

- contact one of the three credit reporting companies (Equifax, Experian, or TransUnion);
- tell the company he or she is a victim of an identity theft and request that a fraud alert be placed on his or her credit report (this initial fraud alert will last for 90 days);
- ask the company to report this request to the other two credit reporting companies; and
- order his or her free credit report (by creating the fraud alert, the victim is entitled to one free copy from each credit reporting company within 12 months of placing the alert).

## STEP 2 – Create an Identity Theft File

Victims should maintain one central file that contains all relevant documentation concerning the fraud. This file is for the victims to maintain only and should be kept in a secure location.



### TAKING ACTION: Victim Recovery CHECKLIST

Help victims track their progress with fraud-specific checklists at:

- > [www.VictimsofCrime.org/taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists)

#### FREE CREDIT REPORT

[AnnualCreditReport.com](http://AnnualCreditReport.com) is the only official source for free credit reports.

Federal law requires each of the three nationwide consumer credit reporting companies—Equifax, Experian and TransUnion—to give consumers a free credit report every 12 months, if asked.

#### CREDIT REPORTING COMPANIES

##### EQUIFAX

(800) 685-1111  
[www.equifax.com](http://www.equifax.com)

##### EXPERIAN

(888) 397-3742  
[www.experian.com](http://www.experian.com)

##### TRANSUNION

(800) 916-8800  
[www.transunion.com](http://www.transunion.com)

<sup>1</sup> Adapted from the Federal Trade Commission's "Identity Theft: A Recovery Plan." Download or order hard copies online at [www.bulkorder.ftc.gov/publications/identity-theft-recovery-plan](http://www.bulkorder.ftc.gov/publications/identity-theft-recovery-plan).

The file should include:

- a timeline of identity theft events;
- the police report, if any;
- the FTC Identity Theft report (See Step 4);
- the victim's most recent credit report from all three credit reporting companies;
- the victim's Internal Revenue Service identity theft affidavit (See Step 8);
- any evidence of the identity theft;
- all written or email communication with creditors, banks, financial institutions, or credit reporting companies; and
- logs of any phone conversations, with dates, names and phone numbers of representatives to whom the victim spoke, and notes on what information was given.

### STEP 3 – Know Your Rights

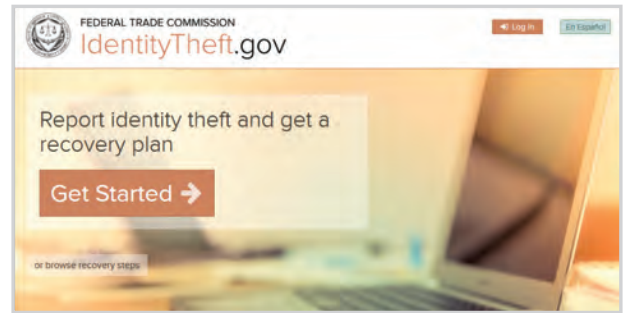
Victims of identity theft have rights created by federal and, in some cases, state law. Victims need to know their rights to protect themselves.

- For federal victim rights, victims can review the Federal Trade Commission's information at [www.identitytheft.gov/know-your-rights](http://www.identitytheft.gov/know-your-rights).
- For state victim rights, victims can check with their state Attorney General, whose contact information is available at [www.naag.org](http://www.naag.org).

### STEP 4 – Report Identity Theft and Build a Recovery Plan at IdentityTheft.gov

Visit IdentityTheft.gov, the Federal Trade Commission's (FTC) one-stop resource for identity theft victims. The interactive website takes victims through the process step-by-step, or victims can browse all recovery steps.

> **Federal Trade Commission's IdentityTheft.gov**  
[www.identitytheft.gov](http://www.identitytheft.gov)



- After completing the complaint process, the victim should print the FTC Identity Theft report.
- This report may be used by local law enforcement to create a police report.
- Once completed, this report remains in the FTC's database and is entered into the Consumer Sentinel Network, which is used by agencies to track and investigate financial fraud.
- ***This step, while important, will not initiate a criminal investigation. The FTC does not resolve individual consumer complaints.***

### STEP 5 – Report the Identity Theft to Law Enforcement

After receiving an FTC Identity Theft report, the victim may ask the local police department to create a police report documenting the identity theft allegation. Ask for a copy of the police report, if possible.

The victim will need to bring:

- the FTC Identity Theft report,
- government identification,
- proof of address,
- any other proof of the identity theft.

The FTC Identity Theft report will create a record that can be used with creditors, banks, credit reporting companies, and other financial institutions to officially corroborate that the identity theft has occurred.

After contacting the local police, the victim can contact the following:

- **District Attorney** – Contact the local District Attorney’s Office.
- **Attorney General** – Contact the Attorney General’s Consumer Protection unit and the prosecution unit to report the fraud. Find the contact information at [www.naag.org](http://www.naag.org).
- **Federal Law Enforcement** – Contact the local FBI Field Office or submit an online tip at <http://tips.fbi.gov>. Look up the local field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field).

## STEP 6 – Consider Placing an Extended Fraud Alert and/or Credit Freeze

Once the FTC Identity Theft report and police report are obtained, the victim is advised to request an extended fraud alert with the three credit reporting companies. This alert will require companies issuing credit in the name of the victim to verify that the victim is actually attempting to open a line of credit.

- Contact all three credit reporting companies separately.
- Use the identity theft report (the combination of the police report and FTC Identity Theft report) to create an extended fraud alert:
  - » The extended fraud alert is free.
  - » The extended fraud alert is good for seven years.

- » The extended fraud alert entitles the victim to two free credit reports from all three of the credit reporting companies within 12 months of placing the extended alert.

- If permitted in the victim’s state, the victim should consider placing a credit freeze on his or her credit report. A credit freeze prevents companies from checking someone’s credit, making it more difficult for fraudsters to use the victim’s identity to obtain credit.

## STEP 7 – Order Three Free Credit Reports

Once an extended fraud alert is created, the victim is entitled to free credit reports from each of the credit reporting companies.

The victim should:

- call all three credit reporting companies, inform them of the fraud alert, and request a free copy of his or her credit report; and
- ask each company to show only the last four digits of the victim’s Social Security number on the report.

## STEP 8 – Contact the Internal Revenue Service

Even if the victim does not think the identity theft is related to his or her taxes, it is possible that the victim’s Social Security number could be used to file fraudulent tax returns. The IRS provides assistance in cases involving identity theft.

- › **IRS Identity Protection Specialized Unit**  
(800) 908-4490



## STEP 9 – Contact the Social Security Administration

If the victim suspects his or her Social Security number has been misused, he or she should call the Social Security Administration to report the misuse.

➤ **Social Security Administration Fraud Hotline**  
 (800) 269-0271 | (866) 501-2101 (TTY)  
 P.O. Box 17785  
 Baltimore, MD 21235

## STEP 10 – Dispute Fraudulent Activity

If any of the perpetrator’s fraudulent efforts were successful, the victim will need to take the following steps, broken down by category:

<p><b>Check Fraud/ Bank Account Identity Theft</b></p>	<ul style="list-style-type: none"> <li>• Contact any financial institution where the victim has a checking or savings account or where the victim’s identity was used to fraudulently open such an account.                             <ul style="list-style-type: none"> <li>» Close these accounts, fraudulent or otherwise.</li> <li>» Ask the bank to report the identity theft to check verification services.</li> </ul> </li> </ul>
<p><b>Credit Card Identity Theft</b></p>	<ul style="list-style-type: none"> <li>• Contact the relevant banks or credit card companies to dispute fraudulent charges.                             <ul style="list-style-type: none"> <li>» Carefully read account statements regularly to look for fraudulent charges.</li> </ul> </li> </ul>
<p><b>Fraudulent Loan or Other Debt Identity Theft</b></p>	<ul style="list-style-type: none"> <li>• Contact the credit reporting companies as well as the companies that issued the credit to dispute any fraudulent lines of credit in the victim’s name.</li> <li>• Contact any debt collector for a fraudulent debt within <b>30 days of receiving notice</b>.</li> <li>• Use copies of the police report, FTC Identity Theft report, and any other documents to assist in this process.</li> <li>• Obtain copies of any documents used to apply for credit or make charges in the victim’s name.</li> <li>• Contact the credit reporting companies and file a dispute about fraudulent activity on the victim’s credit report.</li> </ul>
<p><b>Medical Identity Theft</b></p>	<ul style="list-style-type: none"> <li>• Request from your health insurance company a copy of a listing of benefits that were paid to date.</li> <li>• Examine records from medical and pharmacy providers for accuracy and request corrections, as needed. File a complaint at the U.S. Department of Health and Human Services at <a href="http://www.hhs.gov/ocr/hipaa">www.hhs.gov/ocr/hipaa</a> if the request to review or correct your medical records is refused. Consumers have a right to correct their medical records.</li> </ul>

Sample letters for contacting banks and other companies are available from the FTC at [www.identitytheft.gov/sample-letters](http://www.identitytheft.gov/sample-letters).

## STEP 11 – Consider Civil Remedies

Victims should be aware that the best potential for recovery of lost assets may be through a civil lawsuit. They should be encouraged to consult with civil attorneys who work for victims of financial fraud. The attorney can analyze the particular facts and circumstances of the victim's case and counsel the victim on the available civil remedies. The National Crime Victim Bar Association can provide referrals to attorneys who litigate on behalf of victims of crime and who offer initial consultations at no cost or obligation.

There are several potential civil options for victims of identity theft:

- Many states have laws that allow the victim to directly sue the identity thief.
- A business or organization that failed to properly secure the victim's personal information may be held liable if the perpetrator used that information to steal the victim's identity.
- Banks may be held liable for failing to prevent identity thieves from opening a checking account in the victim's name.
- Under the Fair Credit Reporting Act, credit reporting agencies may be required to pay damages to victims for failing to add an identity theft annotation to the victim's credit report.

### › **National Crime Victim Bar Association**

2000 M Street, NW, Suite 480

Washington, DC 20036

(844) LAW-HELP

Questions can also be emailed to

[victimbar@ncvc.org](mailto:victimbar@ncvc.org).

## STEP 12 – Follow Up

Review all the steps taken and follow up with each agency contacted to encourage progress and report any new developments.



# Investment Fraud Action Steps

Recovery from investment fraud requires victims to take many steps on their own behalf. Victims need to keep complete records to document what has happened. They need to file complaints with the appropriate agencies and know what to expect when they contact these agencies. The information below provides useful guidance for victims of investment fraud.

## STEP 1 – Create an Investment Fraud File

Investment fraud victims should start by collecting all relevant documentation concerning the fraud in one file that's kept in a secure location.

The file should include:

- a contact sheet of the perpetrator's name, mail and email addresses, telephone numbers, and website address, as well as any of the fraudster's purported regulatory registration numbers;
- a timeline of fraud events, which may span many years;
- the police report, if any;
- the victim's most recent credit report from all three credit reporting companies;
- any evidence of the fraud including account statements;
- logs of any phone conversations, with dates, names and phone numbers of representatives to whom the victim spoke, and notes on what information was given; and
- any other relevant documentation concerning the fraud.



### TAKING ACTION: Victim Recovery CHECKLIST

Help victims track their progress with fraud-specific checklists at:

- > [www.VictimsofCrime.org/taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists)

## STEP 2 – Know Your Rights

Victims of crime have rights imparted by federal and, in some cases, state law. Victims need to know their rights to protect themselves.

- For federal victim rights, the U.S. Department of Justice provides information on victim rights and financial fraud at [www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud](http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud).
- For state victim rights, victims can check with their state Attorney General, whose contact information is available at [www.naag.org](http://www.naag.org).
- The North American Securities Administrators Association (NASAA) publishes the following "Investor Bill of Rights": [www.nasaa.org/2715/investor-bill-of-rights](http://www.nasaa.org/2715/investor-bill-of-rights).

## STEP 3 – Report to Regulators

Investors have several options for resolving securities-related disputes. They may contact the brokerage firm involved in the securities-related dispute, file a claim in arbitration, pursue settlement through mediation, file a complaint with a securities regulator, including FINRA, or contact the FINRA Office of the Whistleblower. Investors should be aware that in the case of

investment fraud, in particular, their money may not be recoverable. Learn more about the investor’s options at

[www.finra.org/optionsforinvestors](http://www.finra.org/optionsforinvestors).

The entities below are the national, federal, and state regulatory agencies for investment products and professionals. The victim may benefit from reporting the fraud to as many agencies as apply.

*If complaint involves:*

*Contact:*

<p><b>Brokers and Brokerage Firms</b></p>	<ul style="list-style-type: none"> <li>&gt; <b>Financial Industry Regulatory Authority (FINRA)</b> FINRA Securities Helpline for Seniors: (844) 574-3577 <a href="http://www.finra.org/complaint">www.finra.org/complaint</a> – for complaints against known brokers or firms <a href="http://www.finra.org/fileatip">www.finra.org/fileatip</a> – for tips related to suspected fraud</li> <li>&gt; <b>State Securities Regulator</b> North American Securities Administrators Association: (202) 737-0900 <a href="http://www.nasaa.org">www.nasaa.org</a> – search for specific state contact information</li> </ul>
<p><b>Investment Adviser Representatives and Firms, and Investment Products</b></p>	<ul style="list-style-type: none"> <li>&gt; <b>U.S. Securities and Exchange Commission</b> (800) SEC-0330   <a href="http://www.sec.gov/complaint.shtml">www.sec.gov/complaint.shtml</a></li> <li>&gt; <b>State Securities Regulator</b> North American Securities Administrators Association: (202) 737-0900 <a href="http://www.nasaa.org">www.nasaa.org</a> – search for specific state contact information</li> </ul>
<p><b>Salespeople and Products Dealing in Commodities, Futures, Options, Binary Options, Forex</b></p>	<ul style="list-style-type: none"> <li>&gt; <b>National Futures Association</b> (312) 781-1300   <a href="http://www.nfa.futures.org/basicnet/complaint.aspx">www.nfa.futures.org/basicnet/complaint.aspx</a></li> <li>&gt; <b>U.S. Commodity Futures Trading Commission</b> (866) 366-2382   <a href="https://forms.cftc.gov/Forms/TipsAndComplaints.aspx">https://forms.cftc.gov/Forms/TipsAndComplaints.aspx</a></li> </ul>
<p><b>Insurance Agents and Products</b></p>	<ul style="list-style-type: none"> <li>&gt; <b>National Association of Insurance Commissioners</b> (866) 470-6242 <a href="http://www.naic.org/index_consumer.htm">www.naic.org/index_consumer.htm</a> – search for specific state information</li> </ul>
<p><b>Fraud over the Internet</b></p>	<ul style="list-style-type: none"> <li>&gt; <b>Internet Crime Complaint Center</b> A partnership between the FBI and the National White Collar Crime Center <a href="http://www.ic3.gov">www.ic3.gov</a></li> </ul>

## STEP 4 – Report the Fraud to Law Enforcement

Contact local law enforcement, the local FBI Field Office, and the state Attorney General to file a complaint about the investment fraud with each agency. Reporting the investment fraud to law enforcement is important to begin the recovery process, ensure the responsible parties are investigated, and prevent further damage to other individuals.

- **Local Law Enforcement** – Contact a local law enforcement office to file a police report. Ask for a copy of the police report, if possible.
- **District Attorney** – Contact the local District Attorney’s Office.
- **Attorney General** – Contact the Attorney General’s Consumer Protection unit and the prosecution unit to report the fraud. Find the contact information at [www.naag.org](http://www.naag.org).
- **Federal Law Enforcement** – Contact the local FBI Field Office or submit an online tip at <http://tips.fbi.gov>. Look up the local field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field).

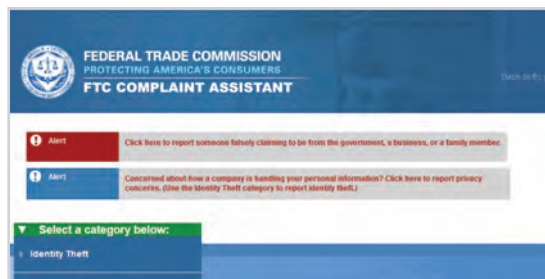
## STEP 5 – Report the Fraud to the Federal Trade Commission

To file a report with the Federal Trade Commission (FTC), contact the FTC’s Complaint Assistant. Lodging a complaint will also enter the fraud into the Consumer Sentinel Network so that law enforcement can track these crimes. (Note, however, that this process will not initiate a criminal investigation.)

### > Federal Trade Commission Complaint Assistant

(877) FTC-HELP

[www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov)



## STEP 6 – Consider Civil Remedies

Victims should be aware that the best potential for recovery of lost assets may be through a civil lawsuit. They should be encouraged to consult with civil attorneys who work for victims of financial fraud. The attorney can analyze the particular facts and circumstances of the victim’s case and counsel the victim on the available civil remedies. A victim can also consider filing an arbitration claim with or without an attorney if a securities broker is involved in the fraud.

The National Crime Victim Bar Association and the Public Investors Arbitration Bar Association ([www.piaba.org](http://www.piaba.org)) can provide referrals to attorneys who litigate on behalf of victims of crime or injured investors, respectively, who may offer the victim an initial consultation at no cost or obligation.

### > National Crime Victim Bar Association

2000 M Street, NW, Suite 480

Washington, DC 20036

(844) LAW-HELP

Questions can also be emailed to

[victimbar@ncvc.org](mailto:victimbar@ncvc.org).

In addition, some law schools provide services to victims in the form of investor advocacy or securities arbitration clinics. Search the SEC ([www.sec.gov/answers/arbclin.htm](http://www.sec.gov/answers/arbclin.htm)) or FINRA websites ([www.finra.org/findanattorney](http://www.finra.org/findanattorney)) for a list of clinics.

## STEP 7 – Follow Up

Victims should keep close track of their case files.

### ASSET FORFEITURE

Returning assets to victims of crime is a top priority of the **Department of Justice Asset Forfeiture Program**.

During the past decade, the victim compensation program has returned more than **\$5 billion in forfeited assets** to victims, through the granting of petitions for remission, or by transferring forfeited funds to courts for payment of restitution through restoration.

For more information, please visit the Department's website at:

[www.justice.gov/criminal-mlars/victims](http://www.justice.gov/criminal-mlars/victims)

# Mortgage and Lending Fraud Action Steps

Recovery from lending fraud requires victims to take many steps on their own behalf. Victims need to keep complete records to document what has happened. They need to file complaints with the appropriate agencies and know what to expect when they contact these agencies. The information below provides useful guidance for victims of lending fraud.

## STEP 1 – Create a Lending Fraud File

Lending fraud victims should start by collecting all relevant documentation concerning the fraud in one file that's kept in a secure location.

The file should include:

- a contact sheet of the perpetrator's name, mail and email addresses, telephone numbers, and website address, as well as any of the fraudster's purported regulatory registration numbers;
- a timeline of fraud events;
- the police report, if any;
- the victim's most recent credit report from all three credit reporting companies;
- any evidence of the fraud;
- logs of any phone conversations, with dates, names and phone numbers of representatives to whom the victim spoke, and notes on what information was given; and
- any other relevant documentation concerning the fraud.



### TAKING ACTION: Victim Recovery CHECKLIST

Help victims track their progress with fraud-specific checklists at:

> [www.VictimsofCrime.org/  
taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists)

## STEP 2 – Know Your Rights

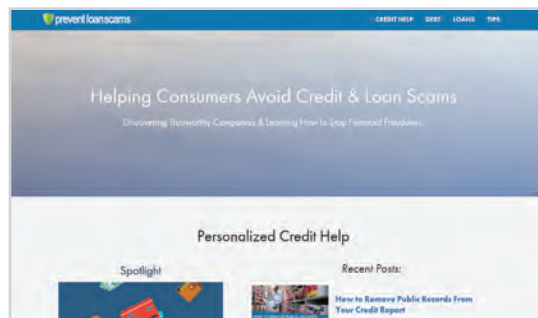
Victims of crime have rights created by federal and, in some cases, state law. Victims need to know their rights to protect themselves.

- For federal victim rights, the U.S. Department of Justice provides information on victim rights and financial fraud at [www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud](http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud).
- For state victim rights, victims can check with their state Attorney General, whose contact information is available at [www.naag.org](http://www.naag.org).



## STEP 3 – Report to the Appropriate Agencies

The victim can benefit from reporting the fraud to as many agencies as apply. For instance, if the fraud was mortgage fraud, the victim should report both to the state agencies responsible for that type of crime and to the Inspector General for the U.S. Department of Housing and Urban Development.



*If complaint involves:*

*Contact:*

State Agencies for All Types of Fraud	> Look up the agency to report to at <a href="http://www.preventloanscam.org/states">www.preventloanscam.org/states</a> .
Mortgage Fraud	> Housing and Urban Development (HUD) Office of the Inspector General (800) 347-3735   <a href="mailto:hotline@hudoig.gov">hotline@hudoig.gov</a>
Mortgage Loan Modification Fraud	> Consumer Financial Protection Bureau (CFPB) (855) 411-2372   <a href="http://www.consumerfinance.gov">www.consumerfinance.gov</a>
Any Lending Fraud	> Federal Trade Commission Complaint Assistant (877) FTC-HELP   <a href="http://www.ftccomplaintassistant.gov">www.ftccomplaintassistant.gov</a>

## STEP 4 – Report the Fraud to Law Enforcement

Contact local law enforcement, the local FBI field Office, and the state Attorney General to file a complaint about the lending fraud with each agency. Reporting the lending fraud to law enforcement is important to begin the recovery process, ensure the responsible parties are investigated, and prevent further damage to other individuals.

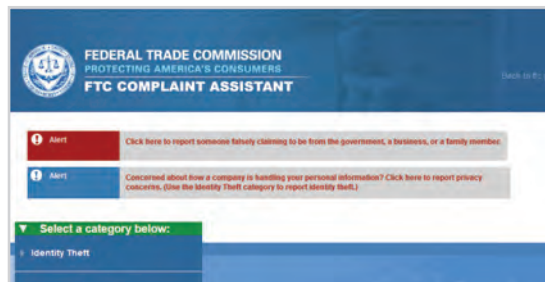
- **Local Law Enforcement** – Contact a local law enforcement office to file a police report. Ask for a copy of the police report, if possible.

- **District Attorney** – Contact the local District Attorney’s Office.
- **Attorney General** – Contact the Attorney General’s Consumer Protection unit and the prosecution unit to report the fraud. Find the contact information at [www.naag.org](http://www.naag.org).
- **Federal Law Enforcement** – Contact the victim’s local FBI Field Office or submit an online tip at <http://tips.fbi.gov>. Look up the local field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field).

## STEP 5 – Report the Fraud to the Federal Trade Commission

To file a report with the Federal Trade Commission (FTC), contact the FTC’s Complaint Assistant. Lodging a complaint will also enter the fraud into the Consumer Sentinel Network so that law enforcement can track these crimes. (Note, however, that this process will not initiate a criminal investigation.)

- › **Federal Trade Commission Complaint Assistant**  
(877) FTC-HELP | [www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov)



## STEP 6 – Contact a Housing Counselor (If Mortgage Related)

The U.S. Department of Housing and Urban Development provides housing counselors for individuals buying a home, refinancing a home, or attempting to avoid foreclosure. All victims of mortgage lending fraud should contact a local housing counselor.

Find a local housing counselor at [www.hud.gov/program\\_offices/field\\_policy\\_mgt/localoffices](http://www.hud.gov/program_offices/field_policy_mgt/localoffices) or call the Housing Counselor Referral line at (800) 569-4287.

## STEP 7 – Treat the Loan Fraud as Identity Theft

Because loan fraudsters may have information pertaining to the victim’s identity, including his or her Social Security number, the victim will need to visit [www.identitytheft.gov](http://www.identitytheft.gov) and should also consult the Identity Theft Action Steps in this guide to:

- establish fraud alerts at all three credit reporting companies; and
- obtain copies of recent credit reports.

## STEP 8 – Consider Civil Remedies

Victims should be aware that the best potential for recovery of lost assets may be through a civil lawsuit. In some cases civil lawsuits have been used to remove liens from victim’s homes and provide victims with good title to their homes. They should be encouraged to consult with civil attorneys who work for victims of financial fraud. The attorney can analyze the particular facts and circumstances of the victim’s case and counsel the victim on the available

### FREE CREDIT REPORT

[AnnualCreditReport.com](http://AnnualCreditReport.com) is the only official source for free credit reports.

Federal law requires each of the three nationwide consumer credit reporting companies—Equifax, Experian and TransUnion—to give consumers a free credit report every 12 months, if asked.

### CREDIT REPORTING COMPANIES

#### EQUIFAX

(800) 685-1111  
[www.equifax.com](http://www.equifax.com)

#### EXPERIAN

(888) 397-3742  
[www.experian.com](http://www.experian.com)

#### TRANSUNION

(800) 916-8800  
[www.transunion.com](http://www.transunion.com)

civil remedies. The National Crime Victim Bar Association can provide referrals to attorneys who litigate on behalf of victims of crime and who offer initial consultations at no cost or obligation.

> **National Crime Victim Bar Association**

2000 M Street, NW, Suite 480

Washington, DC 20036

(844) LAW-HELP

Questions can also be emailed to

[victimbar@ncvc.org](mailto:victimbar@ncvc.org).

## STEP 9 – Follow Up

The victim should continually follow up with each agency contacted to encourage progress and report any new developments.

# Mass Marketing and Other Fraud Action Steps

Recovery from mass marketing and other fraud requires victims to take many steps on their own behalf. Victims need to keep complete records to document what has happened. They need to file complaints with the appropriate agencies and know what to expect when they contact these agencies. The information below provides useful guidance for victims of mass marketing and other fraud.

## STEP 1 – Create a Mass Marketing or Other Fraud File

Mass marketing fraud victims should start by collecting all relevant documentation concerning the fraud in one file that's kept in a secure location.

The file should include:

- a contact sheet of the perpetrator's name, mail and email addresses, telephone numbers, and website address, as well as any of the fraudster's purported regulatory registration numbers;
- a timeline of fraud events;
- the police report, if any;
- the victim's most recent credit report from all three credit reporting companies;
- any evidence of the fraud such as emails, marketing materials and account statements;
- logs of any phone conversations, with dates, names and phone numbers of representatives to whom the victim spoke, and notes on what information was given; and



### TAKING ACTION: Victim Recovery CHECKLIST

Help victims track their progress with fraud-specific checklists at:

- > [www.VictimsofCrime.org/taking-action-checklists](http://www.VictimsofCrime.org/taking-action-checklists)

- any other relevant documentation concerning the fraud.

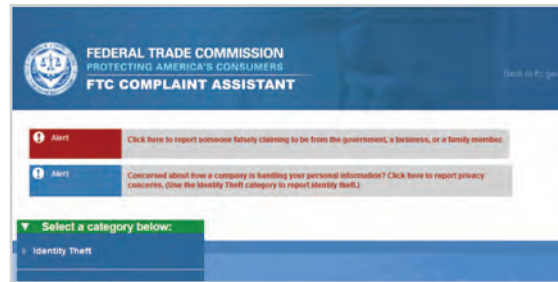
## STEP 2 – Know Your Rights

Victims of crime have rights created by federal and, in some cases, state law. Victims need to know their rights to protect themselves.

- For federal victim rights, the U.S. Department of Justice provides information on victim rights and financial fraud at [www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud](http://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud).
- For state victim rights, victims can check with their state Attorney General, whose contact information is available at [www.naag.org](http://www.naag.org).

## STEP 3 – Report the Fraud to the Federal Trade Commission

To file a report with the Federal Trade Commission (FTC), contact the FTC’s Complaint Assistant. Lodging a complaint will also enter the fraud into the Consumer Sentinel Network so that law enforcement can track these crimes. (Note, however, that this process will not initiate a criminal investigation.)



- > **Federal Trade Commission Complaint Assistant**  
 (877) 438-4338  
[www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov)

## STEP 4 – Report to the Appropriate Agencies

It is important to report mass marketing fraud, no matter the amount in question. The more reports that are made, the easier it is for authorities to hold the perpetrators accountable. Depending on whether the fraud was perpetrated by mail, using wire transfers, or over the Internet, report to the following agencies:

<i>If complaint involves:</i>	<i>Contact:</i>
Consumer Scams	<ul style="list-style-type: none"> <li>&gt; <b>Fraud.org</b> – a project of the National Consumers League <a href="http://www.fraud.org">www.fraud.org</a></li> <li>&gt; <b>Better Business Bureau’s Scam Tracker</b> <a href="http://www.bbb.org/scamtracker">www.bbb.org/scamtracker</a></li> </ul>
International Scams Targeting U.S. Citizens (at Home or Abroad)	<ul style="list-style-type: none"> <li>&gt; <b>U.S. Department of State</b> <a href="https://travel.state.gov/content/passports/en/emergencies/scams.html">https://travel.state.gov/content/passports/en/emergencies/scams.html</a></li> </ul>
Mail Fraud (including Foreign Lottery Scams)	<ul style="list-style-type: none"> <li>&gt; <b>U.S. Postal Inspection Service</b> (877) 876-2455   <a href="https://postalinspectors.uspis.gov">https://postalinspectors.uspis.gov</a> Online Reporting Form: <a href="https://postalinspectors.uspis.gov/contactus/filecomplaint.aspx">https://postalinspectors.uspis.gov/contactus/filecomplaint.aspx</a></li> </ul>
Wire Transfer, Internet-Based Fraud (Cyber-Crime), or Romance Scams	<ul style="list-style-type: none"> <li>&gt; <b>Internet Crime Complaint Center</b> A partnership between the FBI and the National White Collar Crime Center <a href="http://www.ic3.gov">www.ic3.gov</a></li> <li>&gt; <b>Your State Attorney General</b> <a href="http://www.naag.org">www.naag.org</a></li> </ul>

## STEP 5 – Report the Fraud to Law Enforcement

Contact local law enforcement, the local FBI Field Office, and the state Attorney General to file a complaint about the suspected fraud with each agency. Reporting the fraud to law enforcement is important to begin the recovery process, ensure the responsible parties are investigated, and prevent further damage to other individuals.

- **Local Law Enforcement** – Contact a local law enforcement office to file a police report. Ask for a copy of the police report, if possible.
- **District Attorney** – Contact the local District Attorney’s Office.
- **Attorney General** – Contact the Attorney General’s Consumer Protection unit and the prosecution unit to report the fraud. Find the contact information at [www.naag.org](http://www.naag.org).
- **Federal Law Enforcement** – Contact the victim’s local FBI Field Office or submit an online tip at <http://tips.fbi.gov>. Look up the local field office at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field).

## STEP 6 – Consider Civil Remedies

Victims should be aware that the best potential for recovery of lost assets may be through a civil lawsuit. They should be encouraged to consult with civil attorneys who work for victims of financial fraud. The attorney can analyze the particular facts and circumstances of the victim’s case and counsel the victim on the available civil remedies. The National Crime Victim Bar Association can provide referrals to attorneys who litigate on behalf of victims of crime and who offer initial consultations at no cost or obligation.

Even if a victim’s individual losses may not be large enough to make a civil law suit feasible, in cases of mass-marketing fraud where there are multiple victims, those collective losses may make a civil suit a more practical option.

### > National Crime Victim Bar Association

2000 M Street, NW, Suite 480  
Washington, DC 20036  
(844) LAW-HELP

Questions can also be emailed to

[victimbar@ncvc.org](mailto:victimbar@ncvc.org).

## Step 7 – Follow Up

The victim should continually follow up with each agency contacted to encourage progress and report any new developments.



# Section 4 **Prevention** for Victims





# Prevention for Victims

Victims of financial fraud are vulnerable to revictimization. This can happen because personal identifying information is being shared by perpetrators, or because victims are looking for other ways to recover money that they had previously lost. Victim advocates should consider all financial fraud victims as potential future victims. Below are brief tips to help victims prevent financial fraud, broken down by category, with directions on where to find more in-depth information.



Part of your recovery is preventing something like this from happening again. I want to give you some resources to help you protect yourself from fraudsters and prevent future scams.

## Identity Theft Prevention Tips

---

### Protect Yourself:

- Keep all personal and financial records in a locked storage device or in a password-protected electronic file.
- Shred all paper with identifying information before disposing of it.
- Use caution at stand-alone ATM kiosks, gas pumps, and other places where credit cards are often swiped.

### Stop:

- When someone requests your Social Security number, ask if you can provide alternate information. At medical offices, use an identifier that is not your Social Security number.

### Check:

- Monitor bank and credit card accounts weekly.
- Regularly monitor your credit reports. A free copy from each of the three major credit reporting companies is available every 12 months through [www.annualcreditreport.com](http://www.annualcreditreport.com).
- Review the information at [www.safechecks.com](http://www.safechecks.com) to find out how to order safer checks.

## Investment Fraud Prevention Tips

### Protect Yourself:

- Learn to recognize the red flags of persuasion in sales pitches. Start at [www.SaveAndInvest.org/protectyourmoney](http://www.SaveAndInvest.org/protectyourmoney).
- Reduce exposure to sales pitches and use care with free lunch or dinner seminars.
- Develop a “refusal script.”
- Read and save financial account statements, and verify information is consistent with your records:
  - » Investments are as expected.
  - » Any trades were authorized, and the dates align with your notes.
  - » Fees are disclosed and as expected.
- Assess your tolerance for risk. Can you afford to lose some or all of the amount you invested?

### Ask:

- Before working with a broker or other financial salesperson, ask:
  - » Who licensed you to sell financial products? Are you a licensed broker? If not, why not?
- Before buying an investment product:
  - » Is this investment registered with the U.S. Securities and Exchange Commission (SEC)? What are the risks? What could go wrong?

### Check:

- Before working with a financial salesperson verify that they are indeed licensed with the registering agency and that their license is up to date. Check the licensing status, employment history, and disciplinary history (if any) of:
  - » Brokers and brokerage firms using FINRA BrokerCheck: [www.finra.org/brokercheck](http://www.finra.org/brokercheck)
  - » Investment advisers using the SEC’s Investment Adviser Public Disclosure Database: [www.investor.gov](http://www.investor.gov)
  - » Brokers, firms and investment advisers by contacting your state securities regulator: [www.nasaa.org](http://www.nasaa.org)
  - » Insurance agents by contacting your state insurance regulator: [www.naic.org](http://www.naic.org)
- Before buying an investment product: verify that the investment is registered with the SEC. Go to [www.investor.gov](http://www.investor.gov). If you were informed the investment is not registered, learn how you can verify information with a third party that does not have a vested interest in the investment.

### IDENTIFYING FRAUDSTERS

Help victims learn to spot red flags and resist the high-pressure tactics associated with many fraudulent offers:



Order a free DVD of the award-winning documentary from the FINRA Investor Education Foundation, **Trick\$ of the Trade: Outsmarting Investment Fraud** at [www.SaveAndInvest.org/tricks-of-the-trade](http://www.SaveAndInvest.org/tricks-of-the-trade)

## Mortgage and Lending Fraud Prevention Tips

---

### Protect Yourself:

- Don't make a false statement on your loan application, such as overstating your income.
- Never sign a blank document or a document containing blank lines.
- Read all documents before signing.
- If you don't understand what you're signing, hire an attorney to review the documents for you.

### Stop:

- If the terms of a loan sound too good to be true, they probably are.
- Resist high-pressure tactics. Tell the sales person you need time to consider your decision.

### Check:

- Get referrals to loan and mortgage professionals when you want to obtain a loan or mortgage.
- Verify the licenses of mortgage and loan professionals with state, county, or city regulatory agencies.
- Find a housing counselor through the U.S. Department of Housing and Urban Development at (888) 995-HOPE.
- Beware of "no money down" and "no doc" loans. "No doc" loans do not require borrowers to provide documentation of their income. Take extra care to check out the source of these loans with a housing counselor.

## Mass Marketing and Other Fraud Prevention Tips

---

### Protect Yourself:

- Take your name off of solicitation lists.
  - » Direct mail and email offers: [www.dmchoice.org](http://www.dmchoice.org)
  - » Credit card offers: [www.optoutprescreen.com](http://www.optoutprescreen.com) or (888) 567-8688
  - » Online cookie collecting: [www.networkadvertising.org](http://www.networkadvertising.org)
  - » Telemarketing Calls: [www.donotcall.gov](http://www.donotcall.gov).
  - » Block Robocalls: [www.nomorobo.com](http://www.nomorobo.com)
- Shred suspicious mail.
- Get all offers in writing.

### Stop:

- Be cautious when any salesperson solicits you, instead of you seeking them.
- Don't do business with anyone who solicits your money in advance of awarding a prize.
- Don't deposit checks sent by companies that claim the check is for fees or taxes on lottery winnings.
- Don't participate in foreign lotteries. It is against the law.
- Don't respond to junk mail.

### Check:

- Check the credentials of sellers with unbiased, third-party sources, if possible.

- Check with your state business licensing agency (names vary) to verify that the service provider is properly licensed.
- Check with your local Better Business Bureau to see if there are any related complaints.

# Section 5 Resources by Fraud Type



# Resources by Fraud Type

## General Fraud Reporting and Prevention Resources

---

- > Anti-Fraud Hotline for Seniors to Report Fraud  
[www.aging.senate.gov](http://www.aging.senate.gov) | (855) 303-9470
- > AARP Fraud Watch Network  
[www.aarp.org/fraudwatchnetwork](http://www.aarp.org/fraudwatchnetwork)
- > Better Business Bureau  
*BBB Scam Tracker*  
[www.bbb.org/scamtracker](http://www.bbb.org/scamtracker)  
*BBB Scam Tips*  
[www.bbb.org/scamtips](http://www.bbb.org/scamtips)
- > Consumer Financial Protection Bureau (CFPB)  
[www.consumerfinance.gov](http://www.consumerfinance.gov)
- > Elder Justice Initiative, U.S. Department of Justice  
[www.justice.gov/elderjustice](http://www.justice.gov/elderjustice) | (800) 677-1116
- > Federal Trade Commission Complaint Assistant  
[www.ftccomplaintassistant.gov](http://www.ftccomplaintassistant.gov)  
(877) 438-4338
- > Financial Fraud Enforcement Task Force  
[www.stopfraud.gov](http://www.stopfraud.gov)
- > FINRA Investor Education Foundation  
[www.SaveAndInvest.org](http://www.SaveAndInvest.org)
- > Internet Crime Complaint Center  
[www.ic3.gov](http://www.ic3.gov)
- > National Adult Protective Services Association  
[www.napsa-now.org/get-help/help-in-your-area](http://www.napsa-now.org/get-help/help-in-your-area)  
(202) 370-6292
- > National Center for Victims of Crime  
[www.victimsofcrime.org](http://www.victimsofcrime.org)
- > National Center on Elder Abuse  
<https://ncea.acl.gov>
- > National Crime Victim Bar Association  
[www.victimbar.org](http://www.victimbar.org) | (844) LAW-HELP
- > National Consumers League  
[www.fraud.org](http://www.fraud.org) | (800) 876-7060
- > National Network to End Domestic Violence's (NNEDV) "Moving Ahead Through Financial Management Curriculum"  
<https://nnedv.org/mdocs-posts/moving-ahead-through-financial-management>
- > OnGuardOnline.gov  
[www.onguardonline.gov](http://www.onguardonline.gov)
- > Public Investors Arbitration Bar Association  
[www.piaba.org](http://www.piaba.org)
- > VictimConnect Resource Center  
[www.victimconnect.org](http://www.victimconnect.org) | (855) 4-VICTIM



## Identity Theft Resources

---

- > Annual Credit Report (free)  
[www.annualcreditreport.com](http://www.annualcreditreport.com)
- > Federal Bureau of Investigation  
[www.fbi.gov/investigate/white-collar-crime/identity-theft](http://www.fbi.gov/investigate/white-collar-crime/identity-theft)
- > Federal Trade Commission's IdentityTheft.gov  
[www.identitytheft.gov](http://www.identitytheft.gov)
- > Identity Theft Resource Center  
[www.idtheftcenter.org](http://www.idtheftcenter.org)
- > Internal Revenue Service Identity Protection Specialized Unit  
[www.irs.gov/uac/identity-protection](http://www.irs.gov/uac/identity-protection)  
(800) 908-4490
- > National Crime Prevention Council  
*Identity Theft Prevention*  
<http://archive.ncpc.org/topics/fraud-and-identity-theft.html>
- > National Identity Theft Victims Assistance Network  
[www.nitvan.org](http://www.nitvan.org)
- > National Opt-Out Hotline  
[www.ftc.gov/privacy/protect.shtm](http://www.ftc.gov/privacy/protect.shtm)  
(888) 5-OPT-OUT | (888) 567-8688
- > OnGuardOnline.gov  
[www.onguardonline.gov](http://www.onguardonline.gov)
- > Social Security Administration Fraud Hotline  
[www.ssa.gov/fraudreport/oig/public\\_fraud\\_reporting/form.htm](http://www.ssa.gov/fraudreport/oig/public_fraud_reporting/form.htm)  
(800) 269-0271 | (866) 501-2101 (TTY)
- > U.S. Postal Inspection Service  
*Identity Theft Site*  
<https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx>

## Investment Fraud Resources

---

- > Federal Bureau of Investigation  
[www.fbi.gov/stats-services/publications/securities-fraud](http://www.fbi.gov/stats-services/publications/securities-fraud)
- > Financial Industry Regulatory Authority (FINRA)  
[www.finra.org/investors](http://www.finra.org/investors)  
[www.finra.org/brokercheck](http://www.finra.org/brokercheck)  
(844) 574-3577 — *FINRA Securities Helpline for Seniors*
- > FINRA Investor Education Foundation  
[www.SaveAndInvest.org](http://www.SaveAndInvest.org)
- > National Futures Association  
[www.nfa.futures.org](http://www.nfa.futures.org)
- > North American Securities Administrators Association – for state-specific information  
[www.nasaa.org](http://www.nasaa.org) | (202) 737-0900
- > Securities Investor Protection Corporation  
[www.sipc.org](http://www.sipc.org) | (202) 371-8300
- > U.S. Commodity Futures Trading Commission  
[www.cftc.gov](http://www.cftc.gov) | [www.smartcheck.gov](http://www.smartcheck.gov)  
(866) FON-CFTC | (866)-366-2382
- > U.S. Securities and Exchange Commission  
[www.investor.gov](http://www.investor.gov)  
[www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml)  
(800) SEC-0330

## Mortgage and Lending Fraud Resources

---

- > Consumer Financial Protection Bureau  
[www.consumerfinance.gov](http://www.consumerfinance.gov)
- > Federal Bureau of Investigation – Mortgage Fraud  
[www.fbi.gov/investigate/white-collar-crime/mortgage-fraud](http://www.fbi.gov/investigate/white-collar-crime/mortgage-fraud)
- > Federal Trade Commission  
[www.consumer.ftc.gov/topics/homes-mortgages](http://www.consumer.ftc.gov/topics/homes-mortgages)
- > Homeowner’s Preservation Foundation  
[www.995hope.org](http://www.995hope.org)
- > Loan Modification Scam Alert  
[www.loanscamalert.org](http://www.loanscamalert.org)
- > Mortgage Bankers Association  
[www.mba.org/who-we-are/consumer-tools](http://www.mba.org/who-we-are/consumer-tools)
- > National Crime Prevention Council (NCPC) Mortgage Fraud Online Toolkit  
<http://archive.ncpc.org/mortgage-fraud-online-toolkit/about-this-kit/introduction.html>
- > Prevent Loan Scams  
[www.preventloanscams.org](http://www.preventloanscams.org) | (888) 995-HOPE

## Mass Marketing and Other Fraud Resources

---

- > Federal Bureau of Investigation  
[www.fbi.gov/stats-services/publications/mass-marketing-fraud](http://www.fbi.gov/stats-services/publications/mass-marketing-fraud)
- > Federal Communications Commission Consumer Help Center  
[www.fcc.gov/consumers](http://www.fcc.gov/consumers)
- > Federal Motor Carrier Safety Administration – Protect Your Move  
[www.protectyourmove.gov](http://www.protectyourmove.gov)
- > MoneyGram  
<http://corporate.moneygram.com/compliance/fraud-prevention>
- > National Consumers League  
[www.fakechecks.org](http://www.fakechecks.org) | [www.fraud.org](http://www.fraud.org)
- > U.S. Department of State – Resources for Victims of International Financial Scams  
<https://travel.state.gov/content/travel/en/international-travel/emergencies/international-financial-scams.html>
- > U.S. Postal Inspection Service
  - » Criminal Investigations Service Center  
<https://postalinspectors.uspis.gov>  
(877) 876-2455
  - » Delivering Trust  
[www.deliveringtrust.com](http://www.deliveringtrust.com)
  - » Mail Fraud  
<https://postalinspectors.uspis.gov/investigations/MailFraud/MailFraud.aspx>
- > Western Union – Consumer Protection  
[www.westernunion.com/us/en/fraudawareness/fraud-home.html](http://www.westernunion.com/us/en/fraudawareness/fraud-home.html)





[www.VictimsofCrime.org](http://www.VictimsofCrime.org)



[www.finrafoundation.org](http://www.finrafoundation.org)