

Consumer Fraud Reference Guide

This comprehensive guide explains different types of consumer fraud, warning signs, protection strategies, and resources for reporting suspected fraud.

Types of Consumer Fraud

Phishing

Fraudulent emails or messages designed to trick you into providing sensitive personal or financial information.

Example:

An email claiming to be from your bank states there is "suspicious activity" on your account and urges you to "click here immediately" to verify your information. The link leads to a fake website designed to capture your login credentials.

Warning Signs:

- Urgent language demanding immediate action
- Generic greetings (e.g., "Dear Customer") instead of your name
- Poor grammar or spelling errors
- Suspicious sender email address (look closely at the domain)
- Requests for personal information
- Suspicious links (hover over links to see actual destination)

Spoofing

When scammers impersonate legitimate companies, government agencies, or individuals to steal your information.

Example:

A text message appears to come from the IRS claiming you're eligible for a tax refund and includes a link to "claim your refund" that asks for your Social Security number and banking information.

Warning Signs:

- Caller ID showing an official organization but the caller seems suspicious
- Messages from government agencies like the IRS (they typically contact you by mail first)
- Unexpected communications about money or personal information
- Pressure to act quickly
- Requests for payment in gift cards, wire transfers, or cryptocurrency

Catfishing

Creating a false online identity to build relationships, usually with romantic intentions, often for financial gain.

Example:

Someone you met on a dating app or social media claims to have romantic interest but never wants to video chat. After building trust, they share stories of financial hardship or investment opportunities requiring you to send money.

Warning Signs:

- Profile seems too perfect or ideal
- Reluctance or excuses to video chat or meet in person
- Rapid development of intense feelings
- Stories of personal crises shortly after establishing connection
- Requests for money, gift cards, or cryptocurrency
- Vague or inconsistent personal details

Identity Theft

Stealing personal information to open accounts, make purchases, or commit other fraud in your name.

Example:

You receive a credit card bill for an account you never opened, or notice unfamiliar charges on your existing accounts.

Warning Signs:

- Unfamiliar accounts or charges on your credit report
- Missing bills or mail
- Calls from debt collectors about debts that aren't yours
- Denied credit for no apparent reason
- Tax return rejected because one was already filed with your SSN
- Unfamiliar medical bills or insurance rejections

Ponzi/Investment Schemes

Fraudulent investment scams that pay earlier investors with funds from newer investors while promoters steal the majority of the money.

Example:

An "investment advisor" promises guaranteed returns much higher than typical market rates. Initial investors may receive returns (using money from later investors) to create an illusion of legitimacy.

Warning Signs:

- Promises of high returns with little or no risk
- Unregistered investments
- Pressure to recruit friends and family
- Difficulty receiving payments or cashing out

- Overly complex investment strategies
- Investments that aren't registered with the SEC

Credit Repair Scams

Companies that promise to fix credit for a fee but deliver no results or perform services you could do yourself for free.

Example:

A company guarantees they can remove negative items from your credit report for an upfront fee, regardless of whether the information is accurate.

Warning Signs:

- Requests for upfront payment before services are performed
- Promises to remove negative but accurate information from your credit report
- Suggestions to dispute all information on your credit report
- Advice to create a new identity to start fresh with credit
- Lack of explanations about your legal rights

Protection Strategies

1. Know Your Rights

- You have the right to review your credit report annually for free from each of the three major credit bureaus at AnnualCreditReport.com
- You can place free freezes on your credit reports to prevent new accounts from being opened
- You can report fraud to the FTC at ReportFraud.ftc.gov

- Your bank must generally limit your liability for fraudulent transactions if you report them promptly

2. Secure Your Information

- **Use strong, unique passwords** for different accounts - consider using a password manager
- **Enable two-factor authentication** whenever available
- **Be cautious about what you share** on social media - scammers can use this information
- **Secure your mail** to prevent theft of sensitive documents
- **Regularly check financial statements** for unauthorized transactions
- **Use secure, encrypted connections** (look for https) when sharing sensitive information online

3. Verify Sources

- **Never click on links** in unsolicited emails or text messages
- **Contact companies directly** through their official websites or phone numbers (not numbers provided in suspicious messages)
- **Research investment opportunities** thoroughly and verify credentials
- **Be skeptical of unsolicited contacts** - government agencies typically contact you by mail first
- **Verify charity legitimacy** before donating on sites like [Charity Navigator](#)

4. Report Suspicious Activity

- **Report scams to the FTC** at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov)
- **Alert your bank or credit card company** immediately if you suspect fraud
- **File a police report** for identity theft
- **Report investment scams** to the SEC at www.sec.gov/tcr
- **Forward phishing emails** to reportphishing@apwg.org and to the company being impersonated

Steps to Take If You're a Victim of Fraud

1. **Act quickly** - the sooner you address the issue, the better
2. **Document everything** - keep records of all communications, reports, and actions taken
3. **Contact your financial institutions** to secure your accounts
4. **Place a fraud alert** on your credit reports
5. **Change passwords** for all affected accounts
6. **Report the fraud** to the appropriate agencies
7. **Monitor your credit reports** and financial statements closely

For Identity Theft:

1. Visit [IdentityTheft.gov](https://www.identitytheft.gov) to report and get a personalized recovery plan
2. Consider placing a credit freeze with all three major credit bureaus
3. File a police report if your ID has been used for criminal activities

For Financial Fraud:

1. Contact your financial institution immediately
2. Report to the FTC at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov)
3. Monitor your accounts for any additional unauthorized charges

Reporting Resources

Federal Trade Commission (FTC)

[ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov)

For general fraud, identity theft, and unfair business practices

Internet Crime Complaint Center (IC3)

www.ic3.gov

For internet-facilitated criminal activity

Better Business Bureau Scam Tracker

www.bbb.org/scamtracker

To report and search for scams in your area

Securities and Exchange Commission (SEC)

www.sec.gov/tcr

For investment scams and securities violations

Credit Bureaus

Equifax: 1-888-836-6351

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289

To place fraud alerts or credit freezes

Consumer Financial Protection Bureau (CFPB)

www.consumerfinance.gov/complaint

For complaints about financial products and services

Educational Resources

- [FTC Consumer Information](#) - Comprehensive guides, videos, and resources
 - [USA.gov Scams and Fraud](#) - Government resource with prevention guides
 - [OnGuard Online](#) - Tips for online safety and security
 - [IdentityTheft.gov](#) - Recovery plans and resources for identity theft
 - [Pass It On](#) - Resources to help you talk to others about scams
-