





# **Reporting Scams and Fraud to the Federal Trade Commission**

## A Guide for Refugee and Immigrant Service Providers

Refugee and immigrant service providers play a critical role in protecting newcomers from scams and fraud. By encouraging reporting to the <u>Federal Trade Commission (FTC</u>), adopting trauma-informed approaches, understanding <u>common scams targeting immigrants</u>, and offering additional wraparound support, service providers can help clients navigate the challenges they face and empower them to make informed decisions about their financial well-being.

# Recognizing Red Flags and Common Scams

In order to report scams to the FTC, providers must first know how to identify and flag potential scams. This knowledge will help protect clients from losing personal information, money, and property. Even if a client has not personally been affected by a scam, recognizing and reporting scams you encounter can provide valuable information to the FTC and help protect others. Some common red flags include:

- High-pressure tactics: Scammers often create a sense of urgency to trick victims into making hasty decisions.
- Requests for personal information: Scammers frequently request sensitive information such as Social Security numbers, bank account details, or credit card information. Some scammers will ask victims to spell their name and state their address so they can record these details in the victim's own voice and ensure they have the right information to steal the victim's identity.
- Existing knowledge of personal information: Scammers may reveal prior knowledge of their victim's name, address, or place of work. Much of this information is available online, and scammers often rely on these details to create a false sense of legitimacy.

- Upfront fees or payments: Scammers may ask for advance payments or fees for nonexistent services, products, or job opportunities.
- Unprofessional communication: Scammers may use poorly written emails or text messages to communicate with potential victims.
- "Too good to be true" offers: Scammers may promise high returns on investments, lucrative job opportunities, inexpensive housing, or valuable goods at a fraction of their real value. Notably, these offers are often paired with a request for upfront fees or payment.

In addition to these red flags, it is also important for service providers to understand the different types of scams that may target newcomer clients. Some of the most common scams include the following:

- Imposter Scams: Scammers pretend to be someone else, such as a government official, tech support agent, or a loved one in trouble. They often use scare tactics to trick people into sending money or personal information.
- Job Scams: Fake job postings or job offers that require upfront fees, personal information, or payment for training materials and that promise high-paying work-from-home opportunities or easy money for little work.
- Immigration Services Scams: Fraudulent immigration consultants or lawyers who promise to help with immigration paperwork or legal status but often charge exorbitant fees or provide false information.
- Auto Repair or Purchase Scams: Dishonest mechanics or car dealerships that overcharge customers for unnecessary repairs or sell cars with hidden problems.
- Phone Scams: Unsolicited phone calls where scammers try to cheat people out of their money or personal information using various tactics such as posing as government agencies, offering fake prizes, selling fraudulent products, or pretending to be a charity.
- Credit, Debt, or Loan Scams: Fake lenders or debt relief companies that charge high fees or fail to provide promised services.

With a thorough understanding of the red flags and mechanics of common scams, you can empower clients to make informed decisions and reduce the risk of financial harm. Despite these preventative measures, however, scams may still occur. In these cases, it is important to know how to make a report to the Federal Trade Commission (FTC). By reporting scams, service providers can give valuable information to the FTC and prevent these fraudulent activities from affecting others.

## Know the Difference: Federal Trade Commission and Consumer Financial Protection Bureau

The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) are distinct agencies safeguarding consumers in the U.S. The FTC targets unfair and deceptive practices across industries, including false advertising, telemarketing scams, and identity theft. In contrast, the CFPB focuses on financial products and services, ensuring fair treatment by banks and lenders and addressing issues like deceptive credit card practices and predatory lending.

<u>CFPB is committed to ensuring equitable</u> <u>access</u> to their consumer education resources and reporting tool for consumers with limited English proficiency. Service providers can lodge complaints in 180 languages with CFPB <u>here</u>.

Generally, service providers and clients should report broader consumer protection issues to the FTC and finance-specific scams and fraud to the CFPB.

# Making Online Reports to the Federal Trade Commission

The Federal Trade Commission (FTC) is a United States government agency that works to protect and empower consumers by promoting fair business practices and preventing deceptive marketing tactics. Through a variety of resources, such as their <u>Consumer</u> <u>Information page</u>, the <u>Pass It On campaign</u> to protect the digital footprint of older adults, and <u>OnGuard Online</u> for general Internet safety, the FTC strives to educate consumers and service providers on how to secure personal information and resources and make safe, informed financial decisions in the digital marketplace. One of the FTC's key functions is to investigate reports of potential scams and fraud and pursue enforcement actions against wrongdoers. The FTC becomes aware of possible misconduct through reports submitted via their <u>online reporting tool</u>. This tool collects information on the type of scam or fraud that occurred, how the scam was presented to the consumer, the bad actors involved, and any other relevant details. The FTC then uses this information to initiate investigations and act against those who engage in dishonest behavior.

The FTC also leverages the vast pool of reports to detect patterns of unlawful practices and develop educational resources for consumers. These resources provide up-to-date guidance on the latest strategies employed by scammers, as well as tips and strategies for safeguarding against such activities. Visit the FTC's <u>Scam Alerts</u> page for materials you can incorporate into financial literacy programming.

#### **Helping Clients File a Report**

Providers should approach the topic of FTC reporting with sensitivity and respect for clients' backgrounds and past experiences. Some clients may be hesitant to report scams or fraud due to fear of retaliation, mistrust of authorities, or cultural or religious beliefs. Emphasize that reporting is optional, and clients should never feel pressured to report if they are uncomfortable. Set clear expectations by explaining that the FTC cannot directly respond to those who report, and there is no guarantee of a refund if money was lost. Providing clients with all the relevant information empowers them to make informed decisions about their next steps.

If clients opt to report, assist them in gathering necessary information and digital receipts, such as transaction details, email correspondence, or any other documentation related to the scam. You can also support with interpretation, helping clients understand and complete the reporting form, and ensuring all relevant information is included to facilitate a thorough investigation.

Another important aspect of support is helping clients report identity theft, which can be a devastating consequence of scams. It is crucial to recognize the <u>warning signs of identity theft</u>, such as unexplained bank withdrawals, missing bills, rejected checks, unfamiliar accounts on credit reports, and fraudulent medical claims. Being aware of these warning signs allows clients to act quickly, minimizing potential damage and helping them regain control of their personal information. Service providers can direct clients to resources such as <u>IdentityTheft.gov</u>, where they can report identity theft and receive a personalized recovery plan to help them navigate the process of protecting their identity.

#### **Helping Clients Recover Resources**

When a report is submitted, the FTC will send an automatically generated email with information on helping recover lost money, depending on the payment method used. For clients who feel uncomfortable making a report but would like financial restitution, the guidance for recovering funds is summarized below:

- For clients who bought and sent gift cards at the behest of scammers: While gift card funds are the hardest to retrieve, under some circumstances, gift card companies will offer to provide scammed individuals with a refund. Service providers can help clients contact the gift card company and assist them in preparing a statement or gathering necessary documentation. For more information, visit the FTC's guide on gift card scams.
- For clients who sent funds via debit or credit card: Clients should file a dispute or "chargeback" with the credit or debit card company. Service providers can educate clients on their rights and responsibilities when filing a dispute and support them in gathering evidence to strengthen their case. Visit the FTC's guide on disputing credit card charges for more information.
- For clients who provided bank account details or a money transfer: Clients should contact the bank or money transfer company immediately to file a fraud complaint. Service providers can guide clients through the process and provide follow-up support to help the clients open a new bank account if necessary. The <u>FTC's page on money transfer</u> <u>scams</u> provides additional guidance.

#### **Providing Additional Support**

Studies suggest that many asylees experienced extensive insecurity prior to being granted status. They may also have been subjected to torture and/or trauma, and had experiences with authorities who harmed them or failed to protect them. This may foster an ongoing fear over their legal status and mistrust of services. Among asylum-seekers, detention (often over long periods) and fears over the terms of their release represent significant sources of ongoing stress.

Consider working with clients to develop a safety plan to protect their personal information and assets. This may include taking steps such as changing passwords, applying for a new bank account number, ordering and activating a new credit or debit card, and monitoring credit reports for any suspicious activity or unauthorized accounts. The <u>FTC's guide on free credit</u> <u>reports</u> offers more information on this topic.

Depending on the circumstances, clients may also need follow-up financial counseling, debt management assistance, or emergency financial assistance programs. One useful resource is the Consumer Financial Protection Bureau (CFPB)'s "<u>Your Money, Your Goals" toolkit</u>. This comprehensive toolkit offers interactive financial tools, worksheets, and videos to help clients take control of their finances, make informed decisions, and reach their financial goals. "Your Money, Your Goals" is available in multiple languages and can be useful to share with clients to help them build financial literacy and resilience.

## Case Study: Tailored Financial Literacy Program for Refugees and Immigrants

A successful example of a program designed to address scams and fraud targeting refugees and immigrants is the <u>Financial Literacy Program</u> developed by the social work program at George Mason University in collaboration with Catholic Charities USA and AmeriCorps.

The curriculum covers topics such as budgeting, banking, credit, and fraud prevention. The program is contextualized for each service area to address unique needs and challenges faced by the participants. In Camden, NJ, the curriculum was adapted for the financial realities of Syrian women and focused on financial management and credit. In another area, the program was tailored to be taught at an apartment building, making it more accessible to residents. The program's success in building resilient communities demonstrates the importance of contextualizing financial literacy training to address the unique needs of specific populations.

### Conclusion

Through comprehensive support and guidance, you can help clients move forward from experiences with scams and fraud into more secure, stable futures. Familiarizing yourself with red flags and common scams, helping clients file reports and recover resources, and providing additional support when needed are all important steps. By taking a multifaceted approach, providers can play a crucial role in fostering economic empowerment and helping newcomers build stronger, more resilient communities.

To learn more about Switchboard, visit www.SwitchboardTA.org.

The IRC received competitive funding through the U.S. Department of Health and Human Services, Administration for Children and Families, Grant #90RB0052. The project is 100% financed by federal funds. The contents of this document are solely the responsibility of the authors and do not necessarily represent the official views of the U.S. Department of Health and Human Services, Administration for Children and Families.

