COVID-19 Frauds and Scams: *Guide for Housing Counselors*

Due to the COVID-19 national emergency, as well as other disasters and emergencies, scams and frauds are surfacing that target individuals in vulnerable situations. This guide will assist you in helping your clients cautiously navigate suspicious circumstances.

HOW IT WORKS	WHAT CAN YOUR CLIENT DO?
Fraudulent COVID-19 Services and Products	
Your client may be contacted to: ✓ Purchase a vaccine sooner than available under your local government's distribution plan or pay a fee to be placed on a waiting list ✓ Purchase a vaccine that is fake and/or made available through a fake website ✓ Purchase a fake test kit or air filter system ✓ Provide contact tracing information and request personal information like a social security number, address, etc. ✓ Purchase a product that prevents or cures COVID-19 without evidence or proof of effectiveness ✓ Participate in Multi-Level Marketing (MLM) business schemes that offer exaggerated earnings and fabricated health claims ✓ Visit a fraudulent COVID-19 testing site ✓ Receive assistance from scammers with running errands (i.e., picking up groceries, prescriptions, etc.)	✓ Check with your local health department or local government to verify the legitimacy of a COVID-19 vaccine distribution site ✓ Exercise caution when seeking information online. Verify the legitimacy of a website by checking its URL and contact information. For example, a recent scam involved a fake website for the biotechnology company Moderna. The fake URL was "modernatx.shop," very similar to the genuine website's URL "modernatx.com." ✓ Report counterfeit products, services, or companies to The Federal Trade Commission (FTC) for investigation ✓ Check with their local police or health departments to verify the legitimacy of a COVID-19 testing site ✓ Ask for the name of the health care provider offering testing and verify it is a legitimate business ✓ Report suspicious individuals offering errand assistance to their local police department
Government Imposter / Identity Theft	
Your client may be contacted by scammers posing as: ✓ The Internal Revenue Service (IRS) calling to discuss the Economic Impact Payment (EIP) and requesting payment of an advance fee ✓ The Social Security Administration (SSA) calling to notify your client of a payment suspension due to office closures or to request a payment to maintain benefits ✓ The Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO) calling to request donations or sending links via email or text messages that contain malware ✓ The Small Business Administration (SBA) requesting up-front payments related to the Paycheck Protection Program or using phishing attacks to acquire personal information	✓ Stay informed about all EIPs, eligibility requirements, and most recent information at the IRS Economic Impact Payment Information Center. You can still claim a prior EIP (Recovery Rebate Credit), if eligible, by filing a 2020 tax return. This applies to populations who don't normally file, such as people experiencing homelessness or who have very low incomes. ✓ Report suspicious Social Security related calls or scams to the Social Security Office of the Inspector General ✓ Do not open links, attachments, or respond to requests for personal or banking information from unsolicited emails. The WHO and CDC will never contact the general public requesting donations or usernames/passwords. ✓ Do not answer unsolicited calls from the SBA
Unemployment Insurance	
Your client may receive or see: ✓ A notification of unemployment benefits that they did not file for as a result of a fraudulent unemployment claim ✓ Unsolicited emails, letters, calls, or texts, or unauthorized transactions on their bank account or credit card related to unemployment benefits	✓ Contact your local unemployment office about the notification ✓ Report a case of identity theft related to unemployment benefits to your state unemployment office, the IRS, credit bureaus, and your employer's human resources office

Mortgage	
Your client may receive: ✓ A request for up-front fee payments to receive a loan modification or mortgage relief ✓ A request to sign over the title to their property ✓ A request to start or stop making payments to someone other than their servicer or lender	✓ Your client should not open unsolicited emails or text messages from real estate agents, settlement agents, or legal representatives with fraudulent instructions for wiring funds ✓ Avoid answering calls from unknown phone numbers or opening links sent via email or text message ✓ Clients should google important information to verify it
Rentals	
Your client may view: ✓ A fraudulent rental listing requesting a deposit be made before seeing the property ✓ A request for up-front fee payments to receive a rent repayment plan or financial assistance to pay past-due rent ✓ Unsolicited request to join a lawsuit against a landlord to prevent eviction or receive monetary damages	✓ Do not make payments or deposits on a property you have not seen. Verify information about the rental property by searching the property's tax records online ✓ Your client should not open unsolicited emails or text messages from real estate agents, settlement agents, or legal representatives with fraudulent instructions for wiring funds ✓ Avoid answering calls from unknown phone numbers or opening links sent via email or text message ✓ Contact trusted local legal aid resources for reliable information on tenant protections
COVID-19-Charities	
Your client may receive: ✓ A fraudulent call or email soliciting donations to support COVID-19-related efforts ✓ Shared information on social media, such as Facebook or Twitter, asking for donations to fraudulent charities	✓ Do not donate under pressure. Research the organization to ensure its legitimacy ✓ Verify that donations are tax-exempt ✓ Use a credit card instead of a wire transfer or gift card for charitable donations
Social Media or Crowdsourcing	
Your client may view: ✓ Alerts on social media requesting donations for an individual as a result of difficult life events	✓ Research the individual and their situation before donating (Note: Donations to individuals are not tax deductible)
Vulnerable Populations	
Your client may be contacted: ✓ By a scammer posing as a relative or friend in need asking for money and requesting to keep the assistance a secret ✓ By a scammer requesting their Social Security, Medicare, and/or Medicaid number(s). The scammer may use this information to bill these federal health care programs for procedures that were not performed.	✓ Verify the identity of the requestor before sending money and avoid sending money in cash, gift cards, or money orders ✓ Carefully review medical bills and explanations of benefits to ensure the services and dates of service are accurate. Notify their health insurance program if they detect any inconsistencies. ✓ Coordinate with local resources such as the Area Agency on Aging to support vulnerable populations

KNOW THE RED FLAGS	KEEP INFORMATION SAFE
✓ Being asked to give personally identifiable information in an unsecure way ✓ Being asked to send money in cash, gift cards, money orders, or wire transfers ✓ Receiving unsolicited robocalls or texts ✓ Suspicious "Official" notices or signage ✓ Receiving unsolicited offers of "assistance" from unknown sources ✓ Receiving requests for up-front payments for help with programs or loans	✓ Keep your personal information and important papers in a safe place to avoid identity theft ✓ Monitor your accounts regularly ✓ Review your credit report at least once a year or more if you suspect you have been a victim of identity theft. You can get a weekly report at annualcreditreport.com through April 2021 ✓ Use complex passwords ✓ Keep anti-virus software up to date on your computer ✓ Exercise caution when sharing personal information on social media and other websites

REPORT SCAMS

Report scams to the following entities:

- ✓ Local law enforcement or the State Attorney General Office
- ✓ The Federal Trade Commission (FTC) on their FTC Complaint Assistant page and their Identity Theft reporting page
- ✓ The Consumer Financial Protection Bureau complaint page regarding suspicious financial products or services
- ✓ The FBI Internet Crime Complaint Center (IC3) regarding Economic Impact Payments scams
- ✓ The Social Security Office of the Inspector General regarding social security scams
- ✓ One of the three major credit bureaus (Equifax, Experian, and TransUnion) if you suspect you are a victim of identity theft
- ✓ Adult Protective Services and local Departments for Aging regarding scams that target seniors

RESOURCES

Consumer Financial Protection Bureau (CFPB) resources for:

- ✓ COVID-19-related scams
- ✓ Fraud prevention placemats, handouts, and activity sheets for older adults and their families
- ✓ Mortgage Closing Scams: How to protect yourself and your closing funds

Resources to Verify Charities:

✓ BBB Wise Giving Alliance ✓ CharityWatch ✓ Charity Navigator ✓ Tax Exempt Organization Search

Other Resources:

- ✓ The Federal Trade Commission (FTC): Coronavirus Advice for Consumers
- ✓ The Federal Communications Commission (FFC): Coronavirus Scams – Consumer Resources
- ✓ The Social Security Office of the Inspector General: Scam Awareness
- ✓ Centers for Disease Control and Prevention (CDC): COVID-19 Related Phone Scams and Phishing Attacks
- ✓ Department of Homeland Security, United States Secret Service: Know Your U.S. Treasury Check Campaign
- ✓ Small Business Administration Programs: Beware of Scams and Fraud Schemes
- ✓ NeighborWorks: Stop Home Scams