Coping with COVID-19

Avoid pandemic-related ID theft and account fraud

As the nation continues to struggle through the challenges of a pandemic, fraudsters and identity thieves are exploiting the crisis by targeting consumers as they seek information, resources, financial relief, housing assistance and treatment for COVID-19.

This publication highlights some of the most common COVID-related schemes consumers should be on the lookout for, offers tips for protecting yourself, and explains what to do if you should become a victim.

ID theft and account fraud

Identity (ID) theft and account fraud are closely related. Technically, identity theft refers to using stolen information to open and abuse *new* accounts under the victim's name, while account fraud generally refers to misusing someone's personal information to access and abuse the victim's *existing* accounts (also known as "account takeover").

Both identity theft and account takeover are crimes that can have significant consequences. Typically, victims suffer some sort of financial loss. But the consequences can go beyond the monetary, to include effects like erroneous criminal charges or life-threatening healthcare mistakes.

Pandemic-related schemes

Instances of account fraud and identity theft have been increasing for years, but the COVID-19 crisis presented criminals with the opportunity to exploit the unique circumstances of a global pandemic. Widespread fear and uncertainty, combined with newly established relief programs and a nationwide vaccine rollout, created opportunities for fraudsters and thieves.

Some of the most prominent schemes have been:

Unemployment benefits fraud: Personal information gleaned from credit reporting agencies, banks and credit card companies, health insurance systems, and other sources through prior data breaches or identity theft has been used to steal billions in unemployment insurance benefits. Fraudsters file claims using stolen identities, and victims often find out only when their own claims are rejected or delayed, or when they file their tax returns.

Stimulus payments theft: In an effort to get federal stimulus payments to recipients, the IRS launched an online portal (now closed) where eligible Americans who didn't file taxes in 2018 or 2019 could enter basic personally identifying information (name, address, birthdate, Social Security number [SSN], bank account number, driver's license or state-issued ID number, etc.) to register for stimulus payments. Fraudsters who were able to obtain this basic information used it to claim victims' checks. That tool has been closed, but criminals are sure to find new ways to intercept victims' money.

Vaccination-related fraud: The COVID-19 vaccination process has enabled impostors to con people out of their sensitive data—personal information as well as Medicare and health insurance account numbers, etc.—by posing as healthcare or government agency workers doing things like scheduling vaccine appointments. The stolen data has been used to commit a variety of financial and insurance frauds. (Read the fraud alert from the Department of Health and Human Services, offering specific warnings about COVID- and vaccine-related schemes: https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/.)

Rental assistance fraud: Aware that millions of Americans are facing eviction and foreclosure due to pandemic-related job loss, fraudsters are calling, emailing and texting their targets, saying that they are with an agency or program that can provide money for mortgage payments or rent, legal help, or some other service or assistance that would keep them in their homes.

These are just a few of the many fraud and identity theft schemes that have sprouted up since the pandemic began; there are many others that exploit stolen (or unwittingly revealed) data; distress, confusion, hope and need; overwhelmed assistance programs; and consumers' own data security practices.

Safeguarding your data

Making a conscious effort to protect your personal information is the most effective way to avoid becoming a victim. Among the pieces of personal information that can be used to commit ID theft and fraud are your name, address, Social Security number (SSN), birthdate, mother's maiden name, and account numbers (credit card, bank account, Medicare, insurance, driver's license, etc.).

Here are some tips for keeping these and other personal details private:

Social Security number (SSN): Don't carry your Social Security card with you; memorize your SSN. Lower your voice when giving your SSN or other sensitive information in banks, doctors' offices or other public places.

Credit, bank and other cards: Carry only the cards you need that day; if your wallet or purse is lost or stolen, you have fewer accounts in jeopardy. Watch your wallet or purse at all times. Don't hang your purse on your chair in restaurants.

Requests for your information: Never respond to requests for your personal information unless you've initiated the contact or you are absolutely sure you know the company or person you're dealing with. Verify that a request is legitimate by contacting the entity requesting your infor-

mation at the number on your statement or provided by a trustworthy directory or website. Don't click links or open attachments from senders you don't recognize (check the sender's email address carefully).

Documents: Lock your mailbox. Deposit outgoing mail containing checks or personal data in a postal box—don't leave it sitting in your mailbox or apartment lobby. At home, hide sensitive information, like bank and credit card statements, insurance records, etc., where they can't be seen by visitors or workers. Before you discard documents and mail that contain your SSN, account numbers and other personal information, shred them or tear them into tiny bits.

Social media: Remove personal information from your social media accounts, and check your privacy settings to ensure your profile is not publicly visible. Don't post photos of your COVID-19 vaccination card—many have, only to have their identities stolen.

PINs and logins: At teller machines (ATMs), shield the keypad while entering credit and debit card PINS. Don't write down account usernames and passwords; instead, use an online password manager to store your login credentials for different sites—you only have to remember one password in order to access all the others. (Do an online search for "best password managers" to find information and reviews of your options.)

Credit: Placing a freeze on your credit file prevents new credit from being issued in your name. Freezing and unfreezing your reports is free. Learn more in Consumer Action's *Freeze Your Credit File* (https://www.consumer-action.org/modules/articles/freeze_your_credit_file).

Detecting fraud and ID theft

The sooner you catch account fraud or identity theft, the sooner you can stop the damage. Improve the odds of noticing suspicious activity by adopting these practices:

Sign up for fraud alerts. Many creditors and financial institutions offer to send email or text messages to help you spot unauthorized activity on your account.

Monitor your mail. Missing bills, credit card statements and other mail that you expect might mean a crook has taken over your account(s) and changed your billing address. Likewise, if you receive mail you don't expect—like a new credit card you didn't apply for, rejections for credit or loans you didn't apply for, bills or notices you don't recognize, letters (or calls) from debt collectors, etc.—someone may be using your identity to open new accounts.

Check financial statements and bills immediately. Review the statements for your various financial and credit accounts carefully to make sure there is no unauthorized activity. Report anything suspicious to the company immediately.

Check your credit reports regularly. Get free copies from each of the three major credit bureaus (Equifax, Experian and TransUnion) at AnnualCreditReport.com or by calling 877-322-8228. (Through April 20, 2022, you can receive free reports every week, rather than just one per year, upon request.) Review your reports for accounts you don't recognize.

Question credit rejections. If you know you have good credit but your application for new credit is denied, it could signal a problem. Check your credit reports to make sure your credit hasn't been damaged by account activity that is not yours.

Cleaning up the damage

If you discover that you are a victim of account fraud or ID theft, take these steps:

- Visit the **FTC's Identity Theft website** (https://www.identitytheft.gov/) to create an Identity Theft Report and get a recovery plan.
- Consider filing a report with your local police department (if a creditor requires it; you can identify the thief or have specific details that can aid an investigation; or your identity was used in a police encounter). Get a copy of the police report as proof you were victimized. Report the crime to the FBI's Internet Crime Complaint Center (IC3) (https://www.ic3.gov/) if the identity theft occurred online.
- Contact the security or fraud department of each company to dispute any fraudulent transactions and close accounts opened or used without your knowledge. Ask for a letter confirming that the fraudulent account isn't yours, you aren't liable for it, and it has been (or will be) removed from your credit report. Ask if you need to follow up with a written request or statement. (If necessary, request the fraudulent applications and other business transaction records relating to your identity theft, which could help you prove they were forged.)

- Notify **Equifax** (https://www.equifax.com/personal/identity-theft-protection/), **Experian** (https://www.experian.com/help/identity-theft-victim-assistance.html) or **TransUnion** (https://www.transunion.com/blog/identity-protection/know-report-identity-theft) about the identity theft so that they can add a fraud alert to your reports. (Whichever bureau you notify will share the information with the other two.)
- If you suspect that your benefits or tax refund have been stolen, contact the relevant agency (state unemployment office, IRS, etc.) to report the issue and find out what next steps to take to recover the loss.
- Create strong, unique new personal identification numbers (PINs) and passwords for your remaining accounts, even if they haven't been breached.

About Consumer Action

www.consumer-action.org

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

Consumer advice and assistance: Submit consumer complaints to: https://complaints.consumer-action.org/forms/english-form/complaint_form/ or 415-777-9635. (Spanish-language complaints can be submitted to: https://complaints.consumer-action.org/forms/spanish-form/.)

Our hotline accepts calls in Chinese, English and Spanish.

This guide was created as part of Consumer Action's COVID-19 Educational Project.

WELLS FARGO

Funding provided by Wells Fargo