PROTECTING YOURSELF FROM POPULAR SCAM TACTICS

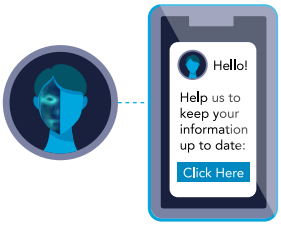
Fraudsters utilize many different tactics to deceive individuals, often to obtain their personal information. This information is then used by fraudsters to create synthetic identities.

Synthetic identity fraud is defined as the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

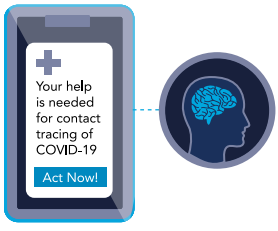
While a fraudster can acquire your personal information through no fault of your own, a common way for fraudsters to get that valuable information is to trick you into giving it to them. They then use it to create a new identity for their own use and to your detriment. This type of deception is often called a "scam," and unfortunately, scams are both extremely prevalent and successful. Below are some potential indicators of scams to help you know what to look for, which could decrease your risk of falling victim to a fraudster's schemes.

COMMON SIGNS OF A SCAM

One aspect of protecting yourself from a scam is to know some of the common signs, or indicators, of one. By understanding these red flags, you can more easily identify a potential scam.



- **Leveraging artificial (or real) familiarity.** A fraudster often pretends to be (or may actually be) someone you know, or from an organization with which you are familiar. Fraudsters will leverage relationships to build your trust and confidence in them and ask for help in some way. This could include asking for your personal information – which they then use for fraudulent purposes – or requesting that you initiate a payment to them.



- **Playing on emotions.** A fraudster will use the natural emotions evoked in certain situations to make you let your guard down. They essentially play to your heart versus your mind. This can be based on both positive and negative emotions. Examples include:

PROTECTING YOURSELF FROM POPULAR SCAM TACTICS

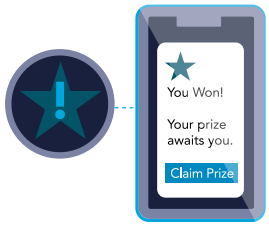
- **Indicating there's a problem.** Fraudsters may use a recent tragedy or world event (e.g., personal hardship, natural disaster, COVID-19 pandemic) to evoke your desire to help. They also may use scare tactics and act as if something will happen to you if you don't act (e.g., your bank account has been compromised or your utilities will be shut off). This plays on the element of fear, which often causes individuals to act quickly versus pausing to evaluate the legitimacy of the situation. In these situations, fraudsters may either ask you directly for money or ask for personal information, which they can then use to create a synthetic identity. If you receive an outreach that points to a problem and an urgent need to act, it may be a scam.

  Example: You are contacted by a company claiming to assist your local government in contact tracing for COVID-19. You are asked to go to their website to enter in your personal information – including name, contact information, Social Security number (SSN) and date of birth. However, this was a fraudster looking to get your personal information to use in synthetic identity creation.

- **Indicating there's a prize or reward.** In this type of example, fraudsters will use positive reinforcement to prompt your action, enticing you with the promise of a perk or reward. Similar to the other example, fraudsters leverage the feeling of excitement evoked by their outreach to cause immediate action on your part, which could lead to an immediate payout from you or providing your personal information which they can use for synthetic identity fraud. If you receive an outreach that seems almost too good to be true, it likely is – so be on the lookout for this scam, as well.

  Example: You receive a call from a company offering you an all-expense paid vacation to the Bahamas. All you have to do is provide your information so they can book your travel for you. They ask for name, contact information, driver's license information, SSN and date of birth. You excitedly hang up the phone awaiting your big trip. Unfortunately, this outreach was from a fraudster looking to get your personal information to use in synthetic identity creation.

PROTECTING YOURSELF FROM POPULAR SCAM TACTICS



- **Encouraging you to click on a link.** This is a common way for fraudsters to either redirect you to a website asking for your information or to download malware to your device, likely exposing your personal information as a result of the malware. Be wary of emails, text messages or instant messaging services (e.g., through social media) that request you to click on a link, as this is likely part of a scam.

COMMUNICATION METHODS USED IN SCAMS

Fraudsters conduct consumer scams using various communication methods, including emails, text messages, phone calls and social media. Here are a few things to look for when receiving communications that also have the scam indicators noted above:

- Always use extra diligence when receiving a communication from an unknown sender.
- If you believe the inquiry may be legitimate, but something seems off, a good practice is to initiate a new, separate outreach using information on the company website or personal contact information you have on file.

LEARN MORE

To learn more ***tips for identifying and avoiding scams***, visit the Federal Trade Commission (FTC) website. Here, you also can find ***additional information on recent scam alerts*** to help stay apprised of identified scams and help prevent you from becoming another victim of those particular scams.

WHAT TO DO IF YOU BELIEVE YOU'VE BEEN SCAMMED

If you think you are a victim of either an attempted or successful scam, you can report this activity via the ***FTC website***.

TAKE ACTION

Being aware of what to look for to identify scams can help protect your personal information and decrease the risk of your information being used in synthetic identity fraud.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.