

What is Identity Theft?

Identity theft is a widespread issue affecting both individuals and institutions which involves the unauthorized use of personal information for fraudulent gain. This may lead to severe financial and legal repercussions for the individual as well as the institution involved. Below are common methods of identity theft with related controls that will help protect you and your organization from identity theft.

Dumpster Diving

- Thieves sift through mail and discarded documents or devices to obtain valuable information.

Proper Disposal of Data

- Information should be disposed of securely per USF or DSO records disposal procedures.

Social Engineering

- A person manipulates individuals into divulging confidential information through methods such as deceptive emails or phone calls.

Education and Awareness

- Stay aware of social engineering tactics and independently verify the authenticity of unsolicited requests even if they appear to be from trusted sources.

Data breaches

- Unauthorized access to sensitive or confidential information, such as personal information, financial data, medical records, or intellectual property.

Strong Passwords and MFA

- Choose strong passwords and enable multi-factor authentication (MFA). Only approve MFA requests when YOU are logging in or performing a secure action.

Where can I find more information?


 USF Office of Internal Audit website: <https://www.usf.edu/audit/>

 [USF Records Disposal Procedures](#) & related Direct Support Organization procedures

How can I report potential fraud or abuse?

 Notify your supervisor.

 Contact the USF Office of Internal Audit at (813) 974-2705.

 Report activities anonymously through the [EthicsPoint](#) hotline at (866) 974-8411.