Developmental Disabilities Administration

Identity Theft

Care Provider Bulletin

October 2018

Did you know?

- Identity theft happens when someone uses another person's personal information to open accounts, file taxes, or make purchases
- Identity theft can happen to anyone
- As a care provider, you can help prevent identity theft from happening to individuals you support

Who is at increased risk?

- Individuals who use social media, such as Facebook, Twitter and Instagram
- Individuals who are more trusting of people they don't know
- Individuals with limited computer skills
- Individuals who are not internet-savvy
- Individuals who rely on others for all support needs

Washington State Department of Social & Health Services

Transforming lives

Prevention

Protect personal and financial information

- Thieves may call or email, pretending they need an individual's personal or financial information. They may make serious threats, state the person is in legal trouble, or the person's services or accounts are in jeopardy. Do not believe them. If they claim to be from a business the individual uses (e.g. person's bank or credit-card company) hang up and call the business to confirm. Some businesses may require personal information to open accounts. Ask the company why they need the information and how they will keep it safe.
- Government agencies, such as the Internal Revenue Service, will not ask for social security numbers or bank information over the phone. If someone calls and claims to be from a governmental organization asking for personal financial information, it is likely a scam.
- Do not provide social security numbers if not necessary. Most times this information is optional. Verify the authenticity of callers by obtaining contact information of the person making the call and calling the company back directly.

Internet safety

- Set up security software for computers, tablets and other devices the individual uses. Set it up to update automatically.
- Use strong passwords difficult for others to guess. If more than one care provider works with the individual, have a safety plan for passwords. Care providers should monitor the accounts to make sure they are not being accessed by anyone unauthorized.
- Encourage individuals who use social media not to accept friend or other requests from strangers; it could likely be a scammer. See if the individual would be willing to review friend requests together to determine authenticity.
- Ask if the individual would like to take an online internet-safety course. Many options are available. Refer to the 'Sources & Resources' section on the second page of this bulletin.
- When using public Wi-Fi; know it may not protect information.
- Use computer security practices from the Federal Trade Commission.

Social safety

- Teach those you support about strangers. Possible scams:
  - Someone will give them money if they provide their personal information.
  - Someone calls or emails with a request to "help transfer funds," and need a bank account number. Such scammers promise money for helping.
- Discourage posting personal information on social media. Thieves can use it to hack into accounts or deceive the person.

Review accounts

- Review credit card and bank statements regularly to check for unauthorized charges. If statements arrive late, call to confirm the billing address and check the account balances to make sure no one accessed them who was not authorized.

Protect information

- Lock financial documents in a safe place
- Lock wallets and purses when possible
- Shred receipts, credit offers, bank statements and other documents or junk mail when no longer needed
- Destroy labels on prescription bottles or medication packs when empty
- Send mail or bill payment from official post office boxes, not a home mailbox
- When mail is delivered to an un-secured mailbox, pick it up immediately

Warning signs

- Unexplained withdrawals from accounts
- Bills or important mail does not arrive
- Calls from debt collectors for other people's debt
- Incorrect information showing up on credit reports
- Medical providers bill for services not used
- Health plan rejects a claim, stating the benefit limit has been reached
- Notification from the Internal Revenue Service that more than one tax return is submitted in their name

When identity theft occurs

- Report identity theft and get a recovery plan through the Federal Trade Commission (FTC).
- The FTC recommends following these steps immediately
  - Call the companies where fraud occurred
  - Place a fraud alert on the accounts
  - Obtain credit reports
  - Report identity theft to the FTC
  - File a report with local law enforcement

Detailed information about each of these steps can be found on the FTC website.

To repair identity theft damage:

- Close new accounts opened in the person's name
- Remove fraudulent charges from the accounts
- Correct the individual's credit report
- Consider adding an extended fraud alert on accounts or credit freeze

Other possible steps:

- Report a misused social security number to the Social Security Administration at 1-800-772-1213.
- Stop debt collectors from trying to collect debts by informing them that the person's identify was stolen (include copies of the identity theft report).
- Replace government-issued forms of identification (e.g. Social Security card, driver's license, state identification card).
- Clear the individual's name of criminal charges by contacting the law enforcement agency that is reporting the crime.
- Contact other offices as needed.

More steps may be needed depending on the type of identity theft - see Federal Trade Commission.

Identity theft can happen to anyone.

Safeguarding information is the key to protection.

Sources & Resources:

- **Video: IdentityTheft.gov Helps You Report and Recover from Identity Theft**, Federal Trade Commission
- **Video: Five Ways to Help Protect Your Identify**, Federal Trade Commission
- **Warning Signs of Identity Theft**, Federal Trade Commission
- **OnGuardOnline: Tips to Help you Stay Safe and Secure Online**, Federal Trade Commission
- Sign up for **scam alerts** from the Washington State Attorney General's Office