Identity Theft and Domestic Violence

What is Identity Theft?

Identity theft is when someone takes a person's identifying information – like their Social Security number, credit card data, or other confidential or sensitive information – and illegally uses it as though it were theirs. Practically, this behavior can include taking over bank and credit card accounts, falsely obtaining credit under someone else's name and credit history, and using this information to buy things like a car. These activities can be devastating to the victim, resulting in lost funds, destroyed credit rating, being accused of crimes committed by the abuser but under the victim's name, and other damage that can take a long time to repair.

Identity Theft in the Context of Domestic Violence

Victims of domestic violence can be particularly vulnerable to identity theft. Survivors of domestic violence often need to take extra precautions to protect themselves from abusers who may use their personal information as a means of control. Their partners have easy access to confidential information that may come to their home in the form of credit card bills and Social Security mailings. Abusers may use such information to open new credit cards in the survivors' names and/or open lines of credit in their children's names. Below are useful tips to help identify if someone is a victim of identity theft and help them to take control of their financial well being and reclaim their financial independence.

How to Find Out if Someone is a Victim of Identity Theft

The victim is typically in the best position to know if his/her identity has been used fraudulently. There are steps a domestic violence victim can take to determine if they have been the victim of identity theft.

- **Review Their Credit Report.** A credit report contains a person's credit history (like loan information and bankruptcies), personal information, as well as a list of entities or individuals who requested that person's credit information. Checking a credit report can help to determine if someone has fraudulently used someone's personal information. A person can obtain their credit report from the three major credit reporting agencies (Equifax, Experian, and TransUnion) either online at www.annualcreditreport.com, or via phone at 1-877-322-8228. You are entitled to receive a free credit report from each of the three (3) major credit reporting agencies once every twelve (12) months.

- **Review Their Bank Records.** Victims of domestic violence should review all of their credit card statements, and other financial documentation carefully to determine if there has been any fraudulent use.

CPB: *5 Empire State Plaza, Suite. 2101, Albany, NY 12223 • Phone (800) 679-1220* ***www.nysconsumer.gov***
OPDV: *80 Wolf Road, Albany, NY 12205 • Phone (518) 457-5800* ***www.opdv.state.ny.us***

Identity Theft and Domestic Violence

How to Prevent Identity Theft

How a victim chooses to protect against identity theft will depend upon her/his unique situation. Any decisions about taking the steps below should be made within the context of an overall safety plan.

- **Open a Post Office Box.** A post office box can protect a person's mail and help to prevent an abuser from getting access to things like pre-approved credit card applications, bank statements, and other information. A victim should make sure this is a safe choice since opening a new post office box for all mail while living with an abusive partner might arouse suspicion.

- **Safeguard Mail.** All unwanted mail that has personal identifying information such as pre-approved credit card offers, retail store charge card offers, and bank statements should be shredded. A victim should send all mail from the post office, not from home. To stop receiving many of the pre-approved credit card offers, they can call 1-800-5OPT-OUT.

- **Protect Social Security Number.** A person should not use their Social Security number as a personal identification number (PIN) or password. A victim may want to consider changing their Social Security number if their abuser knows the number. However, the victim will need to seek direction from the Social Security Administration. To contact the Social Security Administration, call 1-800-772-1213 or visit their website at http://www.ssa.gov/pubs/10093.html.

- **Secure Access to Information.** A domestic violence victim should change passwords and PINs for all accounts on and off-line. She/he should choose complex passwords and PINs that the abuser would not know or figure out. They should not share this information and keep it in a secure location in case it is forgotten.

Responding to Identity Theft

If someone's identity has been used fraudulently, there are steps they can take to address the harm and to correct information on their credit report.

- **Create a Record of Fraud.** A victim can contact local law enforcement to file a police report if they suspect fraudulent use of their personal information. This action may result in a police investigation of the abuser, so the victim should determine if this is a safe choice for them. The victim should check and/or close accounts if she/he feels their identifying information has been compromised. The victim can file a report with the Federal Trade Commission (FTC) at 1-877-ID-THEFT and the Social Security Administration Fraud Hotline at 1-800-269-0271 and/or file copies of police reports or an FTC affidavit with credit bureaus.

- **Security Freezes.** A security freeze placed on a credit report prevents others from getting a copy of the credit report and, as a result, most lenders will refuse to open a new account using that information. This means that an abuser will be less able to open lines of credit in the victim's name because they cannot get access to the credit file without the victim's authorization. Under a new State law, placing and temporarily lifting a security freeze are free for victims of domestic violence. (To be eligible, victims must provide an order of protection, a domestic incident report, a police report, or a signed affidavit from a service provider.)

CPB: *5 Empire State Plaza, Suite. 2101, Albany, NY 12223 • Phone (800) 679-1220* ***www.nysconsumer.gov***
OPDV: *80 Wolf Road, Albany, NY 12205 • Phone (518) 457-5800* ***www.opdv.state.ny.us***

However, be aware that the placement of a Security Freeze could stand in the way of the victim's own needs as well: a security freeze may block getting instant credit, a new credit card, new insurance coverage, or background checks that might be required of a new employer. If the victim needs to permit limited access to her/his credit history for these reasons, she/he must temporarily lift or permanently remove the Security Freeze. A security freeze can be initiated by contacting the three major credit reporting agencies.

- **Fraud Alert.** A fraud alert is a special message on the credit report that informs a lender that there may be fraud involved in the account. It tells creditors to follow certain procedures to verify a victim's identity before extending credit or increasing the credit limit. The fraud alert, however, does not limit access to her/his file. While a fraud alert can help protect against identity theft, it is not as strong a solution as a security freeze. Although it can slow down the person's ability to get new credit, it should not block the person's ability to use existing credit cards or other accounts. A fraud alert can be initiated by contacting the three major credit reporting agencies. A fraud alert can be initiated by contacting the three major credit reporting agencies. An initial fraud alert stays on your file for at least 90 days and can be extended up to seven (7) years provided you submit additional law enforcement records. By placing a fraud alert you are entitled to additional free credit reports.

- **Correct the Credit Report.** If a person thinks that their credit report contains incorrect or incomplete information, they have the right to correct this information. To correct it, send a letter to the credit reporting agencies, along with documentation like credit card statements showing the errors. Make sure it is clear which sections of the report are in dispute.

Other Information and Resources

- **Consumer Protection Board.** For more complete information regarding identity theft, specific instructions regarding security freezes and other remedies, or to file a consumer complaint with the NYS Consumer Protection Board (CPB), call the toll-free hotline at 1-800-697-1220 or visit the CPB's website at www.nysconsumer.gov.

- **Credit Reporting Agencies.**
  - Equifax, P.O. Box 105788, Atlanta, GA, 30348, www.equifax.com, 1-800-685-1111
  - Experian, P.O. Box 9554, Allen, TX, 75013, www.experian.com, 1-888-397-3742
  - TransUnion, P.O. Box 6790, Fullerton, CA 92834, www.transunion.com, 1-800-916-8800

- Privacy Rights Clearinghouse: Nonprofit Consumer Information and Advocacy Organization: www.privacyrights.org
- Identity Theft Resource Center: www.idtheftcenter.org
- Federal Trade Commission: www.consumer.gov/idtheft
- The National Center for Victims of Crime: www.ncvc.org
- US Department of Justice: www.usdoj.gov/criminal/fraud/websites/idtheft.html