Identity Theft Prevention Tips for Job Seekers

PROTECTING YOUR IDENTITY DURING YOUR JOB SEARCH:

- If an employer ask you to write your SSN on your resume or cover letter, ask why it is being requested and explain that you are not comfortable with the request. If it is a required field on an online application, you may enter 000-00-the last four of your social security number.
- If an employer calls you, and during the telephone interview asks for your SSN, do not give it out. Instead, tell them that you will provide personal information when an offer of employment is made and paperwork is completed.

Or

- Let them know that you will contact the company (look it up on the Internet) to provide that information to the Human Resources Department.
- Normally, companies do not do background checks on individuals they have not met. The request for a SSN for that purpose is suspect.
- Be careful about applying for work with a company whose only office seems to be outside of the United States. If you cannot check them out easily with Google search, you may want to look for a job elsewhere.

QUICK TIPS: If an email address does not contain the domain name of the company and is from a personal google/ yahoo/email account, this should serve as a red flag. This does not mean it is definitely fraudulent but it is reason for you to be cautious in your response.

WHEN FILLING OUT APPLICATIONS -

It is recommended that you do not fill in the sections asking for your driver's license number or SSN. Instead, place a note saying "see below." In the blank section at the bottom of the paper, write "Prefer to provide this information during the interview." If asked, you can tell the employer that due to the explosive growth of this crime, you prefer not to include this sensitive information on forms. The reality is that this application may not be safely stored or may be thrown in the trash exposing you to possible identity theft.

DURING THE SCREENING PROCESS -

Companies may require a background check that could include both financial and criminal information. We recommend the following:

- Prior to the background check being done, you will have to provide authorization and specific information for that report to be filed. ONLY provide your authorization and information to a company that you are certain is legitimate.
- Be aware, in advance, of what information is on the report. Your free annual credit report will provide financial information.
- If the criminal record portion will include information that can potentially affect your employability, it is recommended that you be aware of what will appear on that report. You can pull a copy of your report online at https://www.cbirecordscheck.com. Verify for accuracy. If you find an error in your report, contact the reporting agencies ASAP to correct the report.

- If the report provides information that makes you ineligible for hire, ask the employer to see the results. You will not always be provided a copy of the report, therefore, it is extremely important to have knowledge of what will be reported. Try to work with the HR Department to resolve questions/discrepancies.

RESOURCES FOR CHECKING ON AN EMPLOYER -

- Perform a company search on the internet before applying for a job they have posted. You should be able to access the company name, website, address, phone number, type of business, business history, and much more with a simple Google search. This search may also result in newspaper articles, stories in magazines and trade publications, recent promotions, and much more, depending on the size and age of the company.
- Perform an online yellow pages phone number search to verify that any phone number given in the job description is attached to the company.
- The Better Business Bureau publishes a list of client companies that are registered with the BBB, as well as those companies who have negative ratings. Searching their database is a way to identify legitimate companies.
- Other sources that can be helpful in your research are your local Chamber of Commerce, Trade Organizations, City, County, and State Government agencies, U.S. Attorney General and the Federal Trade Commission.

BEST PRACTICE TIPS FOR PREVENTING FRAUD:

- Never give your personal information or credit card number on the phone, through the mail, or over the Internet unless you have initiated the contact and you are sure you know who you are dealing with. Personal information includes: social security number, date of birth, place of birth, home address, driver license number, any account number(s), mother's maiden name and/or passwords.
- Check your credit history and bank records frequently. Look for signs of inaccurate or suspicious activity.
- Keep detailed and accurate records of your banking, check writing, credit card and ATM usage as well as a register that includes all account numbers with contact information.
- Pull a copy of your credit report every year and review closely for accuracy. https://www.consumer.ftc.gov/articles/0155-free-credit-reports Report any discrepancies ASAP.
  The Fair Credit Reporting Act (FCRA) requires each of the nationwide credit reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months. The FCRA promotes the accuracy and privacy of information in the files of the nation's credit reporting companies. The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the FCRA with respect to credit reporting companies.

STEPS TO FOLLOW IF YOU ARE A VICTIM OF IDENTITY THEFT:

If you received a phone call, filled out a form, or gave out information and think you could be a potential victim of a scam, we recommend you take the following steps:

1. **NOTIFY THE POLICE:** File a police report with your local police department stating you have responded to a scam. Provide specific information about what occurred. If you are a victim, this step will be necessary to mitigate your case. Also, you may use this police report to obtain a 7-year fraud alert or a credit freeze.

2. **NOTIFY CREDITORS:** Cancel all credit card, bank account, or ATM/Debt accounts. Obtain new cards for those accounts that are necessary and put a freeze on all other accounts. Report fraudulent activity to credit card issuers. Password-protect those accounts.

3. **CONTACT THE DRIVER'S LICENSE OFFICE:** If driver's license number was also given, contact your local Driver's License office and ask for assistance in determining the best course of action for your situation.

4. **CONTACT THE CREDIT REPORTING AGENCIES:** Contact the credit reporting agencies (CRAs) to place a fraud alert on your credit reports. These are currently 90-day "advisory only" fraud alerts. You may re-establish a fraud alert with the credit reporting agencies on day 91.

FOLLOW-UP STEPS:

1. **MONITOR YOUR CREDIT:** Keep an eye on your credit reports using the annual credit report system by staggering out your requests between the three credit reporting agencies every four months.

2. **REVIEW YOUR ACCOUNT STATEMENTS:** Monitor the monthly statements sent to you from the compromised accounts closely. If there is a questionable charge or change of information then report it to the fraud department of that company immediately and close that account.

3. You may also want to pull a copy of a report from the Social Security Administration to verify all information is accurate and that your SS# is not being used by anyone else. You can access this report as well as other information to verify and protect your Identity at https://www.ssa.gov/myaccount/verifyandprotectid.html

Source: The Identity Theft Resource Center www.idtheftcenter.org