

Business Identity Theft Prevention Checklist

The following tips will help you protect your business, your employees, and your customers from becoming victims of identity theft.

- Create and follow a security strategy in your business plan.
 - Designate a top level manager to implement the plan if you become a victim.
 - If you need assistance in designing a plan, enlist an expert.
- Protect your business records on file with the Colorado Secretary of State by taking the following steps:
 - Assign a trusted person to be responsible for maintaining and monitoring your business record with the Secretary of State.
 - Sign up for e-mail notification about changes to your business record at <http://www.sos.state.co.us/biz/businessFunctionsEmailNotification.do>.
 - Sign up for Secure Business Filing. You can learn more at www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html.
 - Note your annual renewal/periodic reporting date in your business calendar and file the renewal/periodic report on time.
 - File any changes to your business in a timely fashion (such as address, registered agent, name changes, or other changes.)
 - Periodically check your business details on the Colorado Secretary of State's website.
 - If changes have been made without your permission or knowledge, report the fraud to the Colorado Secretary of State immediately, and correct your business record. Please see the "Checklist for Victims" for additional steps to protect your business.
 - Dissolve your business on the Secretary of State's website if you determine that you will no longer be doing business. However, do not unsubscribe from e-mail notification in order to monitor the business record for unauthorized activity.

- Report any lost or stolen credit cards immediately to law enforcement and the credit card provider.
- Monitor your accounts and bills and immediately report any suspicious activity to the originating company.
- Protect your EIN (employer identification number), account numbers, and other personal information.
- Create and follow a policy for carrying, using, and reporting a lost or stolen business credit card.
- Inventory documents that you maintain.
 - Store only those documents you must keep, and keep them in a safe and secure location.
 - If you plan to discard documents, shred them using a cross cut or “confetti” shredder.
- Treat the personal information of your customers and employees with as much concern as you would treat your own.
- Do not share any sensitive information in e-mails or on any Web based service.
 - If you must share sensitive information over the Web, check that the website is secure by looking for “https” in the website address.
- Provide employees with a safe and secure location to keep their personal items (wallets, purses, car keys, etc.) while at work.
- Store employee information such as personnel files, tax, and payroll information in a secure location and limit the number of people who have access to these files.
- Use log-on passwords to protect sensitive information.
- Avoid creating “master” users who have complete access to all of the business’s sensitive information.
- Also check out the “Protecting Your Customers” section of the Business Identity Theft Resource Guide for more information and resources.