



# Business Identity Theft Resource Guide

A Guide to Protecting Your Business and  
Recovering from Business Identity Theft

January 24, 2012

## Contents

---

|  |    |
|--|----|
| Introduction:.....   | 3  |
| Tips on Preventing and Detecting Business Identity Theft .....   | 4  |
| Have a Plan .....  | 4  |
| Protect Your Business Records and Information.....               | 4  |
| Protect Your Business On-line.....                               | 5  |
| Business Records Filed with the Colorado Secretary of State..... | 5  |
| Monitor Activity .....   | 6  |
| Information for Victims of Business Identity Theft .....         | 7  |
| Protecting Your Customers.....                                   | 9  |
| Prevention Checklist.....  | 10 |
| Checklist for Victims .....                                      | 12 |
| Additional Identity Theft Resources .....                        | 14 |
| General Resources .....  | 14 |
| Consumer Resources.....  | 15 |
| Business Resources.....  | 16 |

## Introduction:

---

Identity theft is a crime that affects over 9 million people and costs over \$56 billion to the economy every year, according to the [Better Business Bureau](#). Identity theft impacts many consumers around the country and in Colorado. However, consumers are no longer the only targets of identity thieves.

Business identity theft (also known as corporate or commercial identity theft) is a new development in the criminal enterprise of identity theft. In the case of a business, a criminal will hijack a business's identity and use that identity to establish lines of credit with banks or retailers. With these lines of credit, the identity thieves will purchase commercial electronics, home improvement materials, gift cards, and other items that can be bought and exchanged for cash or sold with relative ease.

The damage can be devastating to the victim's business. The damage to the victim's credit history can lead to denial of credit, which can lead to operational problems. The cost to clean up and correct the damage can be hundreds of dollars and hours of lost time.

The Colorado Secretary of State, the Colorado Attorney General, and the Colorado Bureau of Investigation ID Theft Unit have developed this Business Identity Theft Resource Guide to provide businesses with the information necessary to avoid and reduce the threat of business identity theft and to help those businesses that have already fallen victim to these crimes.

## Tips on Preventing and Detecting Business Identity Theft

The goal of preventing identity theft is to put in place the best possible “lock” to defend against thieves. However, preventing identity theft is like preventing any other crime: there are no 100% foolproof methods to prevent the theft from occurring. If those locks fail, the goal is to detect the theft as quickly as possible so that corrective action can be taken.

The following tips are some of the methods that will help you prevent business identity theft and detect theft in the event that your business’s identity is stolen.

### Have a Plan

A business plan is a critical component of operating and running a successful business. An important, and often overlooked, aspect of a business plan is a security strategy. It is helpful to create a business protection plan that includes steps to prevent and deal with identity theft.

### Protect Your Business Records and Information

Although identity theft can be a high-tech crime affecting those people who shop, communicate, or do business online, the majority of identity theft takes place offline. Stealing wallets and purses, intercepting or rerouting mail, and rummaging through garbage are some of the common tactics that thieves use to obtain sensitive information.

Therefore, it is important to maintain only those records that are necessary to run or operate your business and to shred those records that are not necessary. If you have not done so, take an inventory of the documents that you maintain. The inventory will help you to determine your exposure to risk and manage that risk.

Any documents or records that you must maintain or need to keep to run your business should be maintained in a secure location. You should also limit the amount of mail and paper with financial information printed on it to reduce the chance of criminals stealing it. If possible, you should consider signing up for electronic statements for bank accounts, credit cards, and bills whenever possible.

Never provide an employer identification number (EIN), social security number, financial information, or personal information to anyone unless you have initiated the contact and have confirmed the requesting business or the person's identity.

If a credit or debit card is lost or stolen, cancel the card immediately. Also, if a check is not processed in a reasonable amount of time, contact the payee and consider canceling the check.

Finally, if you reach the point of moving on or retiring from your business and dissolve your business, contact the credit reporting bureaus to notify them that you are closing your business and will no longer be applying for credit.

### Protect Your Business On-line

Do not share financial documents, sensitive personal information, or account numbers via e-mail or other Web-based services. If you must provide this sensitive information over a website, ensure that the site is secure. A secure website is indicated with “https” in the website’s URL.

### Business Records Filed with the Colorado Secretary of State

If you have registered your business with the Colorado Secretary of State, you should do the following:

- Maintain the “Good Standing” or “Effectiveness” of the business;
- Note your reporting or renewal month on a calendar;
- Timely file your reports or renewals;
- Sign up for e-mail notification for your entity or trade name (For more information about e-mail notification, go to [www.sos.state.co.us/biz/businessFunctionsEmailNotification.do](http://www.sos.state.co.us/biz/businessFunctionsEmailNotification.do)); and
- Periodically check your entity’s or trade name’s history.
- Sign up for Secure Business Filing. You can learn more at [www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html](http://www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html).

## Monitor Activity

---

The best method to detect possible identity theft is to monitor activity around your business.

You should:

- Monitor your business's credit report and, if possible, sign up for a credit monitoring service.
- Subscribe to the Colorado Secretary of State's business entity e-mail notifications service at [www.sos.state.co.us/biz/businessFunctionsEmailNotification.do](http://www.sos.state.co.us/biz/businessFunctionsEmailNotification.do).
- Sign up for e-mail alerts for your accounts.
- Monitor your accounts and bills. If an unexpected bill, charge, credit card, or account shows up or a regular bill doesn't arrive, contact the billing company.

## Information for Victims of Business Identity Theft

---

Resolving the problems caused by identity theft is a time-consuming process that will require patience and focus. When resolving identity theft problems, government agencies, financial institutions, and the credit bureaus commonly suggest the following steps:

1. Immediately contact your bank(s) and credit card provider(s).
2. Immediately report any issue to the credit reporting agencies: [Dun & Bradstreet](#), [Equifax](#), [Experian](#), and [TransUnion](#).
  - a. You should speak to the fraud department at each credit bureau. The credit bureaus can put a "fraud alert" on your file that will tell creditors to contact you before they open any accounts in your name.
    - i. [Dun & Bradstreet](#): 1-800-234-3867
    - ii. [Equifax](#): 1-800-525-6285
    - iii. [Experian](#): 1-888-397-3742
    - iv. [TransUnion](#): 1-800-680-7289
  - b. Compare the EIN of the hijacked business to the EIN of your business. Report any discrepancy to the credit reporting agencies.
  - c. You may also want to contact a list of other business credit reporting bureaus. A list of some of the other top business credit reporting bureaus is available at <http://bit.ly/bizcreditbureaus>.
3. File a report with local law enforcement and the [Colorado Bureau of Investigation](#).
4. Contact other creditors and billing companies to notify them of the identity theft.
5. Correct any incorrect information filed with the Colorado Secretary of State by filing a Statement of Correction.

- a. You may wish to include information in an attachment to the Statement of Correction that your business was the victim of identity theft.
6. Document all contacts and take notes about the conversations. Ask for names, department names, and phone extensions, and record the date you speak with each person.
7. Follow up. Make sure creditors and credit reporting agencies receive everything they have requested. It is always a good idea to place a follow-up call or send a letter for confirmation.
8. Don't throw away files. Keep all notes and correspondence in an accessible file in case they are needed in the future.
9. Continue to monitor your accounts and credit report.

## Protecting Your Customers

---

When thinking about identity theft, a business must also think about protecting the personal and sensitive information of its customers. The following resources will help you protect your customers' personal and sensitive information:

“Facts for Business” from the Federal Trade Commission (FTC):

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm>

FTC's Business Identity Theft website:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/business/index.html>

“How to Protect Your Customers” from the Colorado Attorney General's Identity Theft Resource Guide:

[http://www.coloradoattorneygeneral.gov/initiatives/identity\\_theft/how\\_protect\\_your\\_customers](http://www.coloradoattorneygeneral.gov/initiatives/identity_theft/how_protect_your_customers)

“Protecting Personal Information: A Guide for Business” from the FTC:

<http://www.ftc.gov/infosecurity/>

## Prevention Checklist

---

The following tips will help you to 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](http://www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html).
  - Note your renewal/reporting dates in your business calendar and file the renewal/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, don't 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 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.

## Checklist for Victims

---

Resolving issues caused by business identity theft can be a time-consuming and challenging process. The following tips will help you if you are a victim.

- Remember, you are the victim. You are not to blame for the crime.
- Immediately contact your local law enforcement agency or the CBI-Denver Identity Theft Unit at 303-239-4211.
- If you need support, contact the Colorado Bureau of Investigation and request the help of a Victim Advocate.
- Immediately contact your bank(s) and credit card provider(s) and report the theft.
- Contact the largest credit reporting agencies and speak with their fraud departments to report the crime and view your business credit report.
  - Dun & Bradstreet: 1-800-234-3867
  - Equifax 1-800-525-6285
  - Experian 1-888-397-3742
  - Trans Union 1-800-680-7289
- Place a fraud alert on your business accounts.
- Compare your EIN with the EIN of the hijacked business and report any differences to the credit reporting agencies.
- For a list of other business credit reporting bureaus, see the “Information for Victims” section of the Business Identity Theft Resource Guide.
- Contact your business creditors and billing companies, and notify them of the criminal activity perpetrated in the name of your business.
- Contact creditors where fraudulent accounts were opened, and request copies of all documentation used to open or access the account(s).
- Go to the Colorado Secretary of State’s website and correct any fraudulent information by filing a Statement of Correction.

- Attach a copy of a police report and letter from law enforcement, prosecutor, or legal counsel that verifies the identity theft.
- Contact the Secretary of State's Business Division, describe the identity theft, and ask to speak with a supervisor who will assist with correcting your business information.
- Document contacts, including names, titles, phone numbers, and extensions. Include the names and numbers of all law enforcement officers you contact. If you are transferred a number of times, ask the person you eventually speak with for a direct phone number.
- Follow up all calls with a letter (with a return receipt). Also, follow up and make sure that agencies or institutions have received all documents that they need in order to assist you.
- Maintain information. Do not throw away files related to the identity theft. Keep all notes, correspondences, print outs of e-mails, copies of reports, and other documents in a secure and accessible file.
- Monitor your credit report and your business record with the Secretary of State regularly.
  - If you have not already signed up for e-mail notification with the Secretary of State, sign up at <http://www.sos.state.co.us/biz/businessFunctionsEmailNotification.do> now.
  - Sign up for Secure Business Filing. You can learn more at [www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html](http://www.sos.state.co.us/pubs/business/ProtectYourBusiness/secureFiling.html).

## **Additional Identity Theft Resources**

---

The following are important and useful resources for understanding, preventing, and correcting identity theft:

### **General Resources**

---

Colorado Attorney General Identity Theft Resources:

[http://www.coloradoattorneygeneral.gov/initiatives/identity\\_theft](http://www.coloradoattorneygeneral.gov/initiatives/identity_theft)

Colorado Bureau of Investigation Identity Theft Unit:

[http://cbi.state.co.us/inv/ID\\_Theft/Index\\_IDTheft.html](http://cbi.state.co.us/inv/ID_Theft/Index_IDTheft.html)

Identity Theft Resource Center – Colorado resources website:

<http://www.idtheftcenter.org/artman2/publish/states/Colorado.shtml>

Federal Deposit Insurance Corporation (FDIC): <http://www.fdic.gov/consumers/theft/index.html>

FTC's Identity Theft website: <http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>

Identity Theft Victims Advocacy Network:

[http://webstarts.com/sites/0128/rbliss@spike.dor.state.co.us/s\\_1227910257416/index.html](http://webstarts.com/sites/0128/rbliss@spike.dor.state.co.us/s_1227910257416/index.html)

Resources from the Government: [www.identitytheft.gov](http://www.identitytheft.gov)

Social Security Administration: <http://go.usa.gov/iwT>

Social Security Fraud Hotline: 1-800-269-0271. If you suspect that someone is using your Social Security number for fraudulent purposes, call the hotline.

U.S. Department of Justice: <http://www.justice.gov/criminal/fraud/websites/idtheft.html>

U.S. Postal Service: <http://www.usps.com>.

If you believe your mail has been stolen or redirected, notify your local post office.

U.S. Postal Inspection Service: <https://postalinspectors.uspis.gov/>

U.S. Secret Service: <http://www.secretservice.gov/>

## Consumer Resources

---

Experian Credit Freeze Information:

[http://www.experian.com/consumer/security\\_freeze.html#state](http://www.experian.com/consumer/security_freeze.html#state)

Experian Credit Freeze Information for Colorado:

<http://www.experian.com/consumer/help/states/co.html>

The Office of the Comptroller of the Currency (OCC) publication “How to Avoid Becoming a Victim of Identity Theft”: <http://www.occ.treas.gov/idtheft.pdf>

Colorado Department of Public Health and Environment website regarding “Identity Theft and Vital Records”: <http://www.cdphe.state.co.us/certs/idtheft.html>

Social Security Administration publication “Identity Theft and Your Social Security Number”: <http://www.ssa.gov/pubs/10064.html>

Social Security Administration publication “Your Social Security Number and Card”: <http://www.ssa.gov/pubs/10002.html>

Wells Fargo fraud prevention tips:

[https://www.wellsfargo.com/privacy\\_security/fraud/protect/fraud\\_tips](https://www.wellsfargo.com/privacy_security/fraud/protect/fraud_tips)

Wells Fargo online, mobile, computer and e-mail security tips,

[https://www.wellsfargo.com/privacy\\_security/fraud/protect/online\\_tips](https://www.wellsfargo.com/privacy_security/fraud/protect/online_tips)

## Business Resources

---

Bank of America, Small Business Online Community, Play It Safe- How to Protect Your Customers' Confidential Info:

<http://smallbusinessonlinecommunity.bankofamerica.com/blogs/TechnologyManagement/2008/09/30/play-it-safe>

Bank of America, Small Business Online Community, Protect Your Business:

<http://smallbusinessonlinecommunity.bankofamerica.com/blogs/TechnologyManagement/2007/10/21/protect-your-business>

Better Business Bureau, Data Security – Made Simpler: <http://www.bbb.org/data-security/>

Colorado Division of Motor Vehicles:

<http://www.colorado.gov/cs/Satellite/Revenue-MV/RMV/1177024843128>

Call if any of your business's vehicles may have been subjected to identity theft.

FDIC publication “A Crook Has Drained Your Account. Who Pays?”:

<http://www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html>

FDIC publication “Classic Cons”:

<http://www.fdic.gov/consumers/consumer/news/cnsprg98/cons.html>

FDIC publication “Your Wallet: A Loser's Manual”:

<http://www.fdic.gov/consumers/consumer/news/cnfall97/wallet.html>

Federal Trade Commission Red Flags Rule Guidance: <http://ftc.gov/redflagsrule>

Federal Trade Commission Red Flags Rule How-to Guide:

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

Fraud.org, Scams Against Businesses:

<http://www.fraud.org/scamsagainstbusinesses/bizscams.htm>

OCC publication “Check Fraud: A Guide to Avoiding Losses”:

<http://www.occ.treas.gov/chckfrd/chckfrd.pdf>