license or social security number on your checks or allow anyone to write this information on your checks.

- Order a copy of your credit report from one of the three major credit reporting agencies every 3 months. Check each report carefully for signs of unusual activity. The Fair Credit Reporting Act (FCRA) requires each one of these agencies to provide you with a free copy of your credit report once every 12 months. Call toll free 877-322-8228 or visit www.annualcreditreport.com.

- Always place payments in a postal service box or arrange for them to be paid via the Internet. Never place outgoing payments in the mailbox in front of your home.

What To Do If You Have Become A Victim

STEP I: Notify Credit Agencies Contact the following credit reporting companies:

- Trans Union 1-800-680-7289 www.tuc.com
- CSC Credit Services 1-800-272-9281 www.csccredit.com
- Equifax 1-800-525-6285 www.equifax.com
- Experian 1-888-397-3742 www.experian.com

STEP II: Notify merchants and creditors.

STEP III: Review your credit report.

STEP IV: Contact the Federal Trade Commission.

If You Have Been The Victim of Check Fraud

STEP I: Notify your bank.

STEP II: Send checks to your bank.

STEP III: Notify the check-processing companies.

- National Check Fraud Service 1-843-571-2143 www.ckfraud.org
- Telecheck 1-800-710-9898 www.telecheck.com
- Global Payments Check Service 1-866-860-9061 www.globalpay.com
- Consumer Debit Resource 1-800-428-9623 www.consumerdebit.com

STEP IV: Inform merchants

Identity Theft

Stevensville Police Department
102 Main St. Ste D
Stevensville, Mt 59870

Town of STEVENSVILLE POLICE DEPARTMENT

How Identity Thieves Get Your Personal Information

- Stealing wallets and purses containing your identification and credit and bankcards.
- Stealing mail to get new credit cards, bank or credit card statements, new checks, tax information, and pre-approved credit offers.
- Completing a “change of address” form to divert your mail to another location.
- Rummaging through your trash or the trash of a business looking for individual’s personal data in a practice known as “dumpster diving.”
- Obtaining your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for, and legal right to, the information.
- Stealing personal information from your home or from businesses or institutions where you are a customer, patient, employee, etc.
- Obtaining personal information that you share with others over the Internet.
- Scamming you, either by U. S. Mail or e-mail, by posing as legitimate companies or government agencies you do business with. This usually happens after someone gets your information from businesses by stealing files out of offices where you are a customer, employee, patient or student. Sometimes an employee of these businesses is bribed, or files are hacked into via the Internet.
- Copying data from credit and debit cards as the card is being used for a legitimate transaction using a device called a “skimmer”.
- Setting up look-alike web sites for legitimate businesses that you transact with and tricking you into sending personal information by sending e-mails warning that your accounts have been compromised or are about to expire and instructing you to click on a link.
- Standing behind you as you enter your PIN number or credit card number in a practice known as “shoulder surfing”.

What to Do to Avoid Becoming a Victim

- Manage your personal information wisely and avoid disclosure unless absolutely necessary. Remember that your Social Security number is the key to obtaining your credit report and other confidential information. Disclose only when absolutely necessary.
- Keep personal information in a secure place at home. Shred all documents containing identifying data.
- Limit the number of credit and debit cards in your purse or wallet. Never carry documents such as social security cards or birth certificates with you.
- Never disclose personal information in response to a telephone call or an e-mail. Legitimate business that you transact with are never likely to ask for this information. If you are instructed to click on a link contained in an e-mail asking for personal information, visit the organization’s web site instead. Criminals will sometime create authentic looking false web sites for businesses you are already familiar with in order to obtain your information.
- Shield your hand when entering your PIN number at bank ATMs or point of sale terminals. Always take receipts with you and shred them. Never have check orders delivered to your home. Instead, pick them up at the bank yourself. In addition, never print your driver