

## SAFETY SHORTS

### FALL PREVENTION: ENTERING AND EXITING EQUIPMENT

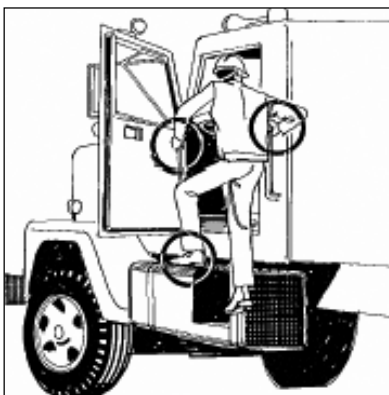
Falling while getting into or out of truck cabs or heavy equipment or when mounting or dismounting truck bodies or trailers can cause serious injuries. Many knee, ankle and back injuries result from jumping from equipment onto uneven ground or objects.

The biggest cause of falls from a vehicle is human error and failure to follow the “Three Point Rule”. The Three Point Rule requires three of four points of contact to be maintained with the vehicle at all times – two hands and one foot, or both feet and one hand. This system allows maximum stability and support, reducing the likelihood of slipping and falling.

There are important steps that can be taken to prevent mounting/dismounting injuries, with use of the Three Point Rule being most important.

#### What the Employer can do:

- Evaluate every truck and piece of equipment. Provide additional steps, non-slip surfaces and hand holds where necessary.
- Maintain steps, contact surfaces and handholds in useable condition. Inspect frequently.
- Instruct all workers in safely mounting and dismounting equipment, including the 3-point contact method.
- Install warning decals or signs in the cab or on the door of trucks and heavy equipment reminding workers to use 3-point contact.



#### What the Operator can do:

- Keep steps, ladders and standing surfaces free of snow, mud and debris. Report damage immediately.
- Don't use tires or wheel hubs as a step surface.
- Don't use the doorframe or door edge as a handhold.
- Wear footwear with good support and slip resistance.
- Don't climb down with something in your hand. Leave it on the vehicle floor and retrieve it after getting safely on the ground.
- Don't rush to climb out after a long shift. Descend slowly to avoid straining a muscle.
- Be extra careful when working in inclement weather.
- Exit and enter facing the cab. Get a firm grip on rails or handles.
- Never Jump! You may land on an uneven surface, off balance or on something. Look before exiting.

A wide variety of Safety Shorts can be found on the MMA website at:  
[www.memun.org](http://www.memun.org)

**\*Always follow the Three Point Rule\***

# WHO ARE YOU?

## Protecting your entity and employees from identity theft

With almost 10 million people victimized each year, identity theft is the fastest growing financial crime in the United States. The total cost of identity theft is estimated at almost \$50 billion a year. The Federal Trade Commission (FTC) reports that individuals lose roughly \$5 billion, with businesses and financial institutions stuck for the rest. The FTC said that in 2003 alone, identity theft victims spent almost 300 million hours resolving their problems. They often found the process bewildering, frustrating and time-consuming.

Identity theft has been the No. 1 fraud complaint for five straight years and anyone can become a target. It happens to customers, businesses and employees. In recent months, banks, online retailers and big brokers of consumer data have revealed breaches in security that placed tens of thousands of Americans at risk of identity fraud.

Identity thieves steal personal information in many ways. Although a study released by the Better Business Bureau reports that lost and stolen wallets, checkbooks and credit cards are the leading sources of ID theft, other common causes are dishonest employees and mail theft. Thieves pick through the trash for pre-approved credit card applications. Professionals who prepare tax returns have been accused of claiming their own client's tax refunds. Online schemes are also a serious problem, costing consumers tens of millions of dollars through identity fraud that includes e-mail scams, computer viruses and spyware programs.

How can you avoid being a victim of identity theft? Nobody can guarantee that you, your business, or your employees won't be targeted. But by managing information wisely, being aware of threats, and educating yourself, you can help yourself, your business and your employees against identity theft and fraud. Here are 10 simple steps that can help you reduce the risk of information being stolen and misused:



**Identity thieves steal personal information in many different ways.**

**1. Order your credit report** - Get credit reports every year from each of the three major credit reporting agencies. We recommend you space the reports out over the year. (See credit agency contact information on the following page.) A convenient resource is [AnnualCreditReport.com](http://AnnualCreditReport.com), which was created by the three major credit agencies as a centralized source of credit information. You can request free reports from each agency through this single Web site. Check each report for accuracy and for indications of fraud, such as credit accounts that you or your business did not open, applications for credit that you or your business did not complete, or credit inquiries that you or your business did not make. Check the identifying information in the credit report to be sure it is accurate including name, address and Social Security number.

**2. Guard your Social Security number** – Don't carry your Social Security card with you; store it in a secure place. Release your number only when necessary, such as on tax forms or employment records. When a business wants your Social Security number, ask to use another number. Don't have your Social Security number printed on checks and don't supply it to merchants who want to write it on your checks. Review your Social Security Earnings and Benefits statement each year to ensure no one is using your number for employment.

**3. Protect your mail from theft** – Mail outgoing bills from post office collection boxes rather than in an unsecured mailbox. Don't leave outgoing mail for your postal carrier to pick up. Pay attention to billing cycles and keep track of incoming mail, particularly tax forms, pay stubs, credit card bills and bank statements. If statements are late, call to find out when the statements were mailed. Pick up new checks at the bank. Consider a locked mailbox and have the post office hold mail when you are away.

**4. Destroy documents before disposal** – Tear, or better yet, shred your charge and ATM receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements. Also, destroy expired credit cards and convenience checks or credit offers you get in the mail. If you do not want mailed credit

offers, contact AnnualCreditReport.com to have your credit reports from all three major reporting agencies market “no solicitation”. (See contact information below.)

**5. Shop online with caution** – Use only a credit card when shopping online, not a debit card. Designate a single, distinct credit card with a low limit for online shopping. Use a secure browser before you provide any credit information over the Internet. To determine if a site is safe, look for the “lock” symbols in the status bar at the bottom of your browser window. Look for the words “Secure Sockets Layer” or the acronym “SSL” in the merchant’s privacy statement. Never send payment information via e-mail.

**6. Keep your computer safe** – Update virus protection software regularly. Download and install security patches for your operating system or browser. Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1, which leaves your computer connected to the Internet 24 hours a day. Before you dispose of a computer, use a “wipe” utility program to overwrite the entire hard drive and make files with personal information unrecoverable. Never store personal information on a laptop computer.

**7. Pick your PINs carefully** – Do not use any part of your Social Security number for any Personal Identification Number (PIN). Don’t use any combination a thief could easily figure out, such as birth dates, a pet’s name, mother’s maiden name, address, telephone number or consecutive numbers. Memorize all your PINs and do not write them down anywhere. Finally, shield the PIN pad when you are entering the number in a retail establishment or at an ATM to prevent others from observing your PIN.

**To Stop Unsolicited Credit offers  
call AnnualCreditReport.com at  
1-888-567-8688**



## CREDIT REPORTING AGENCIES

### **Equifax**

PO Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
www.equifax.com

### **Experian**

PO Box 9532  
Allen, TX 75013  
1-888-397-3742  
www.experian.com

### **TransUnion**

PO Box 6790  
Fullerton, CA 92835  
1-800-888-4213  
www.transunion.com

### **AnnualCreditReport.com**

Request credit reports from all  
three agencies online,  
or call: 1-877-322-8228

## **8. Lock up important documents**

– Keep all documents with personal or account information under lock and key in your home. Always keep your purse or wallet in a safe place at work, preferably in a locked drawer. Carry only cards you need.

**9. Record your credit and bank account information** – List or photocopy all of your credit and debit cards, including the account number, expiration date, credit limit and the telephone numbers of customer service and fraud departments in case your cards are stolen. Make a similar list for your bank accounts.

**10. Don’t take that call** – Don’t give out personal information on the phone, through the mail or over the Internet unless you’ve initiated the contact. Identity thieves may pose as representatives of mortgage companies, banks, credit card companies, Internet service providers and even government agencies to get you to reveal your personal information.

*The foregoing is an abbreviated version of an article written by Mark MacGougan, Assistant Vice President for new product development with The Hartford Steam Boiler Inspection and Insurance Co. Mr. MacGougan manages the company’s identity recovery insurance program. This article, first published in July 2005, has been reprinted with permission from Public Risk Magazine, the official publication of PRIMA (Public Risk Management Association).*

## October 2005 Safety Enhancement Grants

### **\$106,050 Awarded to 89 Applicants!**

By the September 30, 2005 deadline, Risk Management Services received 104 applications for its semi-annual Safety Enhancement Grant review. Applicants included municipalities, schools, water and sewer districts, counties, housing authorities and an incorporated fire department, all of whom were eligible for participation in the Safety Enhancement Grant program by virtue of their participation in the MMA Workers Compensation Fund. The following is a partial list of safety equipment that will be purchased by the awardees:

Body Armor	Gas Detector
Bleacher Workhorse	Hydraulic Tailgate Lift
Chainsaw Safety PPE	Hydrostatic Test Pump
Confined Space Equipment	Magnetic Manhole Buddy
Ergonomic Workstations	Kitchen Mixer Guard
Eyewash Station	Personal Escape Rope Kit
Fireproof Cabinet	Personal Water Rescue Vests
First Aid Station	Riot Helmet
Flammable Liquid Cabinet	Traffic Safety Signs and Vests
Fall Harness Protection	Fire Dept Turnout Gear
Fume Exhaust Unit	TV/VCR for Training

## CONTRATULATIONS TO ALL GRANT RECIPIENTS!

The next Safety Enhancement Grant deadline is

**April 30, 2006**

Applications available online at [www.memun.org](http://www.memun.org)  
For questions about RMS grant programs contact  
Ed MacDonald or Deb Balmer at 1-800-590-5583

Also, be sure to check out the details and application form for the  
**RMS SCHOLARSHIP GRANTS**  
on the MMA Website at [www.memun.org](http://www.memun.org)