



Vacation Protection Tips

Identity theft is often a crime of opportunity. Do not be a vacationer who presents a crook with that opportunity. Your personal information, credit and debit cards, driver's license, passport, and other personal information are the fraudster's target. A few minutes spent planning before you travel can help reduce the risk that a fraudster will ruin your vacation.

Call your bank and credit card companies to let them know when and where you will be traveling.

To guard your identity while vacationing, here are some tips:

- Clean out your wallet. Remove unnecessary credit cards, your Social Security card, and other unneeded documents that could compromise your identity if lost or stolen while on vacation.
- It is best to carry two credit cards. Carrying too many credit cards will subject you to additional aggravation if your wallet is lost or stolen. But there is a risk in carrying only one credit card if, for example, your card inadvertently becomes inactivated due to suspected fraud or if the magnetic strip becomes damaged. Having this happen while away from home could become a major headache.
- Photocopy or make a list of the remaining contents of your wallet. Keep it in a secure and locked location or with a trusted individual at home whom you can contact in case your wallet is lost or stolen.
- Do not leave your wallet or any documents containing personal information in your hotel room unattended. Hotel rooms are not the most secure places. Many people have access to the room. Use a hotel safe when available.
- Call your bank and credit card companies to let them know when and where you will be traveling. Their fraud departments may then monitor your accounts for unauthorized transactions during this



time. It is also recommended that you know your personal identification number (PIN), before traveling, if your PIN is a six digit PIN ask your financial institution to convert it to a four digit PIN that will be more widely accepted while traveling abroad.

- Many countries, including those in Europe, use chip and PIN or EMV-enabled cards, these cards use a microchip and a personal identification number (PIN) embedded in the chip to validate transactions. A U.S. issued credit card without a chip and PIN can still be used while traveling but usually only at locations with a sales attendant. Many locations, such as ticketing machines, toll roads and fuel pumps, require the chip and PIN cards.
- Leave your checkbook in a secure locked place at home.
- Use credit cards instead of debit cards. This reduces your vulnerability to having your checking account emptied while you are on vacation. Debit Cards and Credit Cards have different fraud reporting timelines and liabilities for the consumer, check with your bank to learn more details.

- Guard your credit card receipts and car rental agreements, particularly if they contain your full credit card number.
- If you plan on using an ATM card during your vacation, use one that does not have debit card privileges (for example one that requires a PIN and does not contain a Visa or MasterCard logo). You can ask your bank to change an ATM/debit card to one that is "ATM only." It is best to use ATM machines found at banks or credit unions and that are in well-lit areas. Be sure to examine the ATM machine carefully for signs of tampering. Be on the lookout for anything that looks suspicious; a simple pull of the card reader or a wiggle of the keypad will help identify possible skimming devices or altered ATMs. Also look for small or pin-hole cameras placed above the keyboard that try and steal your PIN. Always remember to cover your hands when you enter your PIN, it's the easiest way to protect yourself from a hidden camera or someone looking over your shoulder.
- When dining at a restaurant, try to keep an eye on your credit card when you pay your bill. If the server removes your card from sight, they may be able to create a "clone" by using a portable card skimmer that will copy the information from the card's magnetic strip.
- Many restaurants have installed table-top payment pads or self-service tablets to allow consumers to pay for their bill right at the table. This could improve credit card security by ensuring your card never leaves your possession, limiting the risk of your card being "cloned" or even accidentally leaving your card at the establishment. Be sure to read the instructions carefully, ask about and "fees" for using the service and ensure your transaction is fully completed and processed prior to leaving.
- Ask your Post Office or a trusted neighbor to hold your mail for you. Mail that is left in an unlocked mailbox is a goldmine for identity thieves. It also sends a signal to potential burglars that your house is vacant.
- If you are bringing your laptop with you, be very careful when using it to access online banking or

other password-protected services from Wi-Fi networks. Be sure to use Wi-Fi "hotspots" that are secured.

- Be aware that keyloggers (software that can track your keystrokes) may be tracking you when using cyber-café, hotel business centers, or other public access Internet facilities rather than bringing your own laptop with you. Public access facilities may use servers that are not encrypted. Therefore, never access any sensitive information from a public computer.
- Always be cautious with the information you share on social networking sites. You would not put a sign on your front door saying "Away on Vacation". When you broadcast your travel plans on a social networking site, you are doing the same thing electronically. This information can then be used by criminals who will know that you will be away from home.
- Turn on two-factor authentication if offered. Two-factor authentication is an added layer of security that combines something you have, a physical token such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53718-8911

Email: DATCPHotline@wi.gov

Website: datcp.wi.gov

Phone: (800) 422-7128 TTY: (608) 224-5058

IDTheftVacation604 (rev 10/23)