NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Guest Column: Identity Thieves Don't Take Vacation

A Commentary from Ben Brancel, DATCP Secretary

Release Date: **June 21, 2016**

Media Contact: **Jerad Albracht, 608-224-5007**
Bill Cosh, Communications Director, 608-224-5020

DATCP Secretary Ben Brancel

MADISON – The summer travel season is underway! As you pack for your adventures, you'll surely check and double-check your luggage for your swimwear, toiletries, clothes and other essentials. But there is another important issue to consider when you are preparing to hit the road: the potential risk to your identity when you are on the go.

Identity theft is often a crime of opportunity. If you let your guard down during your vacation, you may be giving criminals a chance to take advantage of your change in routine and setting.

Thankfully a bit of pre-planning can help protect you from this vulnerability. So, let's get packing!

First things first: money. Consider using a credit card instead of a debit card when possible on your trip. A credit card may offer better protection if your card is lost or stolen. Because a debit card is linked to your checking or savings account, the potential loss could be higher if your information is misused.

For safety's sake, you don't want to take too many credit cards with you, but you also don't want to be stranded if the one card you pack is lost or not working. The vacation sweet spot is two cards. Pack them separately and keep a photocopy of each in a secure place at the hotel (or with a family member back at home) in case you need to call the credit provider to cancel service on a card during your trip.

As you dig out your cards of choice from your wallet, use the opportunity to clear out any unnecessary sensitive documents like banking, identification, Social Security or Medicare cards. Take only what is absolutely necessary.

Once you've picked your cards and cleared your wallet, call your bank and credit card companies to let them know when and where you will be traveling. Their fraud departments can monitor your accounts for unauthorized transactions.

If you pull cash from an ATM during your journey, be on the lookout for skimmers: card reading devices that criminals install on the machine to capture your credit information. Skimmers may be small card readers that fit over the ATM's native reader or they may be devices installed inside the machine to catch the information as it passes through the system. Before you swipe your card, look for signs of tampering on the machine, especially broken security seals or loose card readers. When criminals install skimmers, they may also mount small cameras on or around the ATM to capture you entering your PIN number. Shield the button pad while you enter this information.

Next, let's focus our sights on your electronics. Even if you intend to use your vacation as a way to escape both the real AND digital worlds, you may still pack a smartphone or other web-enabled device for the journey. Take some steps to tighten the security around your device.

Before you do anything else, backup your device so your documents, music, photos and videos are safe at home. Consider removing any files containing sensitive information that you

(MORE)

will not need while traveling, such as your taxes or downloaded copies of bank statements. Once that is complete, enable any tracking and remote storage wiping features on your device and set it to timeout and require a login passkey. On the off-chance that you lose your device, you want to make it as difficult as possible for another party to dig into the system and any remaining sensitive files (and to give law enforcement a chance at tracking it down).

On your adventure, always use caution on public Wi-Fi networks. Only use secure Wi-Fi access points and avoid logging into online banking or other password-protected services from public networks whenever possible. If you use a public computer at an internet café, library or other type of public facility, be especially careful – if there is any malicious software on the device, it could track what you type and your online activities.

Finally, everyone loves to see photos of their loved ones having fun in the sun, but be cautious with the information you share on social networking sites during your trip. You would never put a sign on your front door saying "Away for Vacation," but you are essentially doing just that if your account is set for public access. Log into your social media accounts and tighten the security settings BEFORE you hit the road.

Now that you have taken these simple steps, you can travel with the confidence that you have some protections in place against identity theft during your trip. Have fun and don't forget your sunscreen.

###