NEWS RELEASE

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

Leave Your Worries at Home: Consumer Protection Tips for Spring Breakers

Release Date: **March 8, 2018**

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

MADISON – Spring break is a time for letting go and having fun, and no traveler wants to worry about the risk of getting ripped off by identity thieves while they are kicking back on the beach. The Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) asks travelers to take some simple steps before, during and after their trips to limit their risk of having personal information stolen when they are away from home.

"Scammers don't take vacation, and if you let your guard down on spring break, you could open a door that allows an identity thief to dig into your sensitive accounts," said Michelle Reinen, Director of the Bureau of Consumer Protection. "Taking simple steps like tightening the restrictions on your social media accounts and putting your mail on hold can go a long way toward keeping personal details from getting into the wrong hands while you are on the go."

In the same way you will check and double-check your door locks before you leave the house and start your journey, you should devote a couple of pre-trip minutes to shoring up your online accounts, strengthening the protection around your mobile devices, and limiting your risk of information exposure. While traveling, avoid sharing sensitive information over public WiFi networks and keep the trip details you share on social media accounts to a minimum. When you return home, run an antivirus scan on your devices and update passwords for your social media, email and financial accounts.

Here are additional pre-, during and post-trip tips:

Before you start your trip:

- **Alert your financial institutions.** Call the number on the back of your credit and debit cards and let them know where and when you will be travelling. This advance notice lets the bank know to expect transactions from the areas you visit, keeping your account from being locked.
- **Verify your reservations.** If you booked your trip through a third-party website or travel service, confirm your reservations directly with the airline, hotel or car rental business so you don't get stranded in case of a miscommunication with your booking.
- **Put your mail on hold.** Identity thieves could steal mail from unattended mailboxes, giving them the information they need to misuse your identity and open credit lines in your name. The post office can hold your letters and packages until you return.
- **Limit what is in your wallet.** Don't carry your Social Security card in your wallet or purse and limit the bank cards you take on your trip.
- **Pack a second credit card.** If you lose your main card or it is damaged, you will need a backup. Keep them packed in separate locations.
- **Photocopy your documents and cards.** Make two copies (front and back) of your passport, driver's license, credit cards, tickets and hotel reservation confirmations in case your original documents are lost or stolen during your trip. Give one copy to a friend or family member at home and carry the other copy with you, stored securely and separately from the originals.
- **Share your plans with friends and family to avoid "grandparent scams."** Phone scammers could call your relatives while you are away, claim to be you, and ask for money to get out of a phony legal or medical emergency. Make a family plan that includes the best way to reach you directly if a relative or friend receives one of these frightening calls and set a code word or phrase to use to verify legitimate emergency calls.

(MORE)

- **Tighten the security around your social media accounts.** Your public posts could give a thief the tools to steal your identity or rob your home while you travel. Adjust the security settings on your accounts to only allow friends and family to view your posts, and consider turning off the location services on your phone so the photos you post online are not tagged with GPS data. Make sure that your mobile devices are password protected.

While on vacation:

- **Use caution with public WiFi.** Avoid banking or sharing sensitive data over public WiFi networks. Only send sensitive information over password-protected networks and in secure websites (those that start with "https://" – the "s" stands for secure).
- **Keep personal documents close.** Make use of a room safe when available for mobile devices, valuables and sensitive documents like passports, ID cards, credit cards and airline tickets. Do NOT pack a Social Security card unless it is necessary.
- **Always keep your mobile devices in a secure location.** Your smartphone, tablet and laptop contain a wealth of personal information. Know where these devices are at all times and keep them secure in public. Log out of all websites so your accounts are not accessed if your device is lost or stolen.
- **Don't broadcast your trip on social media.** In sharing your travel plans, you are providing information for scammers to use in their ploys (think "grandparent scams") and for thieves to use in determining when your home is unattended.

When you get home:

- **Change passwords.** Any website you accessed on your trip was fair game for scammers, so change all of your passwords – especially for your email account.
- **Check accounts.** Take a look through your bank and credit card accounts and identify any irregularities. Bring them to the immediate attention of your financial institution.
- **Check credit reports.** Review your credit reports to ensure that no unexpected accounts have been created in your name.

For additional information, visit the Bureau of Consumer Protection at http://datcp.wi.gov, send an e-mail to datcphotline@wisconsin.gov or call the Consumer Protection Hotline toll-free at 1-800-422-7128.

Connect with us on Facebook at www.facebook.com/wiconsumer or on Twitter: @wiconsumer.

###