keen BANK

Identity Theft

TRAVEL SAFE

Travel can be great, but it can also make you extra vulnerable to identity theft. Here are some things you can do to lower your risk.

Reduce What You Carry

Before you leave, clean out your purse and/or wallet. Remove all unnecessary cards or items. Carry nothing with your social security number on it. Make note of which cards and documents you decide to carry in case of loss or theft.

Be On Alert in Tourist Areas

These are favorite payment card skimming spots as well as popular with purse snatchers.

Avoid Using Public or Shared Computers

They could have information-stealing software in place. If you must use one, avoid entering any personal information or logging onto online accounts.

Avoid Taking Your Checkbook

Your checks show your name, address, bank name, checking account number and checking account routing number—a whole "kit" thieves can use to take over your account. They also can forge checks to withdraw money. If you opt not to use cash or payment cards, use traveler's checks.

Verify Callers to Your Hotel Room

A common scam involves a call to your hotel room from the "desk clerk". This person tells you about a problem that requires you to provide a credit card number over the phone. If this happens, hang up and call or visit the front desk to check.

Downsize Delivery Dangers

Thieves slip made-up flyers for fake food delivery services under hotel room doors, hoping you will call and order using your credit card. Check the reliability of all fliers with the front desk.

Be Careful When Using Wi-Fi

Airports, hotels and other public places offer Wi-Fi for Internet access. A secure wireless network encrypts all the information you send using that network. However, Wi-Fi hotspots are often not secure. This measures information you send though some websites or mobile apps can be accessed by other network users. If you choose to use public Wi-Fi, be very cautious.

- Make sure it's an authenticated Wi-Fi network. Always manually select network connections and know the exact name of the establishment's network. Scammers may set up "free" computer-to-computer networks with look-alike names to fool you.
- Never log in or send personal information to unencrypted website and be aware that for security, the site should be fully encrypted.
- Always log off an account as soon as you have finished using it.
- Consider a VPN (virtual private network) service to protect your information when using public Wi-Fi.