TRAVEL SAFETY TIPS

Before you go:

- [ ] Only book through a legitimate agency or website, as there are many travel scams out there. Read the fine print before signing.
- [ ] Pay for your travel arrangements with a credit card - it gives you some control in disputing charges.
- [ ] Stop your mail before leaving so that data thieves aren't opening your financial mail for you.
- [ ] Turn on automatic account alerts on your credit card to easily monitor all transaction (via smartphone) without having to look at statements.
- [ ] Turn on remote tracking and wiping software on your phone so that if it is lost, you can locate and/or wipe the data off from anywhere.
- [ ] Make sure that your laptop computer has long, strong, alpha-numeric password encryption (BitLocker for Windows, FileVault for Mac).
- [ ] Leave most of your identity at home, especially checkbooks, Social Security cards and excess credit and debit cards.
- [ ] Take your passport (if international), driver's license (use this for ID, not your passport), credit card and a dedicated ATM/debit card with enough money in the account to cover your trip. I recommend these as backup and cash as your main form of payment. This limits your exposure to exactly how much you have on you.
- [ ] Make a photocopy of those items, front and back, in case of loss. Take the photocopy with you (store separately) in case you lose your ID.
- [ ] Request a nameless, travel-only ATM/debit card with a 4-digit PIN from your bank.
- [ ] Never post on social network sites that you are leaving (it let's robbers know you aren't home) and refrain from posting pictures on the road until you return. Secure your home as much as possible with lights, locks and alarms.

On the road:

- [ ] Protect your identity and small devices in a travel wallet or secure pocket. Pickpockets can open backpacks and purses without your ever knowing.

- [ ] Free Wi-Fi hotspots are simple for thieves to eavesdrop on. Instead, surf on your cellular data plan (call your provider for international data plans and "tethering" instructions).

- [ ] Never type anything sensitive on a public computer (hotel, cafe, library) as your data is probably being recorded and possibly exploited.

- [ ] Be obsessive about keeping control of your smartphone, as it's a mobile computer connected to your wealth. Turn on the passcode, enable remote tracking and never leave it lying around or loan it out, especially in public.

- [ ] At ATMs, make sure that there isn't a skimming device attached by wiggling anything that sticks out from the machine. Shield your PIN# from those behind you and never let anyone help you get money out, pay for tickets, etc.

- [ ] Lock your digital devices, valuables and traveling papers in your hotel room safe when you don't need them.

- [ ] For added protection, put the privacy sign on your door and let housekeeping know that you don't want service. Unmade beds are better than stolen documents or devices.

- [ ] Never give credit card or other information over the phone in your hotel - many scams look like the front desk calling for your information.

Back home:

- [ ] Review credit card statements for any fraudulent charges that happen after the fact (common).

- [ ] Turn off your dedicated ATM/debit card.

- [ ] Restart your mail and make sure no critical statements are missing.

- [ ] Turn off your international data plan.