

# Data Security and the Worry-Free Traveler

## *Don't Let Identity Theft Ruin Your Summer Travel Plans*

It seems Americans have given up on the true getaway vacation. According to a recent study by Expedia, Americans receive – and use – less vacation time than their European counterparts. And for those who do get away, many often take the office with them on the road. **We simply can't unplug.** Unfortunately, data breaches and identity theft don't take holidays either. Given that the loss of a laptop, thumb drive, or even a wallet is all too common when traveling ... maybe relaxing *too much* isn't such a good thing after all.

*Brian Lapidus, chief operating officer for Kroll's Fraud Solutions, admits to being a bit hyper-connected himself. As the summer travel season heats up, he offers these important tips for a safe journey – whether it's for leisure, business or a little bit of both:*

1. **Lock it up at home.** If you've entrusted the family dog or Aunt Zoe's twenty-year old rubber tree to a caretaker while you're gone, put identity-rich items away before you hand over the house key. Don't leave out tax returns, credit card statements, utility bills and the like. It's human nature to be trusting of others, but front-line experience confirms that a significant percentage of identity theft is perpetrated by someone known to the victim.
2. **Lighten your laptop's load.** Remember, thieves can't steal what you don't have. Before you hit the road, make time to take inventory. Transfer sensitive, confidential data from your laptop to your company's secure central server, or move it to a disk that may be stored safely until you return. Items you'll want to remove whenever possible include personnel files with dates of birth and Social Security numbers, and customer files with identifiable bank or credit card information. Not even your online personal bill-paying programs should make the trip. If you are *required* to have sensitive information with you, consider purchasing an **encrypted** thumb drive and storing the information securely.
3. **Don't tempt fate.** If you must take along your laptop or PDA-berry, treat it like a cache of cash or fine jewelry. If the room safe isn't large enough to hold a laptop, consult hotel or cruise ship management and arrange for storage in a centralized main safe or secure holding area. Locking your laptop in your personal quarters -- no matter how smart a hiding place you contrive -- creates needless exposure and worry.
4. **Block prying eyes with a privacy filter.** Thanks to what's called microlouver technology, laptop users can simply snap privacy filters on over their screens to block viewing from an angle. You can see what's displayed from your primary user vantage point, but onlookers at your left or right are prevented from snooping. Office supply stores sell privacy filters, as do many general retailers; prices range from \$65 to \$150 depending on screen size.
5. **Short-circuit the personal broadcast.** Since 2006, U.S. passports have included RFID (radio frequency identification) chips. Some credit cards use them, too. The continuous transmission of radio waves means that your personal details are being regularly aired, as well. Invest in an RFID-blocking passport case or wallet to jam unintentional reception – and any accidental disclosure of your identity. Search 'RFID-blocking wallet' online and find a host of sources, including familiar sites like Amazon.com and Magellan.com, where prices are comparable to similar high-quality leather goods.
6. **Be quiet.** Cell phones have erased the boundaries between public and private space for many people. Even if you don't intend to listen, it's almost impossible to tune out what's being said just a few feet away. Heighten your *own* awareness about what you say in public – and how loudly you say it. Whether you're talking about a pricey souvenir you just bought or keeping

**Confidential.** This material is CONFIDENTIAL to Kroll's Background Screening Division and Fraud Solutions Practice and may not be reproduced, published, or disclosed to others without the advance written authorization of Kroll.

tabs on a company project, your words can put you and your company at risk if a thief is within earshot.

7. **Beware the Wi-Fi.** One of Kroll's standard tips for businesses also holds true for the average traveler. Use of wireless networks means your data is being transmitted over open airwaves, similar to a radio transmission. If not properly secured, data can easily be picked up by an uninvited party. Earlier this spring, the FBI warned about hackers cruising wireless networks for this very reason. Set your computer default to require your authority before connecting to a new network. And when it does, be sure the address matches what you typed in.
8. **Keep that key.** When you check out of a hotel where you were issued a card-key to unlock the door to your room, don't leave the card-key behind. Hold on to it until you're safely home and can shred or otherwise discard it safely. Some say it's an urban myth that card-keys hold vital details like credit card numbers, while others report having tested and confirmed the presence of private data coded into the magnetic strip. Even if there's no definitive answer, why risk it?
9. **Use public computers at your own risk.** Public computers, like those found in a hotel's business center, can contain "keylogger" spyware, which records every keystroke including passwords and account information. Keyloggers make it possible for an identity thief to steal any information entered into the computer during your session. Conducting important company (or personal) business on a public computer also increases your vulnerability to "shoulder surfers" – individuals who look over your shoulder to observe what you are doing and, more importantly, collect the sensitive data you're entering.
10. **What's in your wallet?** Before you hit the road, make photocopies of the personal material in your wallet: driver's license, credit cards, insurance cards, etc. – front and back – and store those copies in a safe place at home. Should your wallet be lost or stolen, you won't be left wondering what was actually taken, and you'll be able to quickly notify the appropriate agencies about what has taken place. Furthermore, someone at home can always send you the duplicate information you need to get you back to where you want to be -- home.

## About Kroll

Kroll, the world's leading risk consulting company, provides a broad range of investigative, intelligence, financial, security and technology services to help clients reduce risks, solve problems and capitalize on opportunities. Kroll Inc. is a wholly-owned subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC), the global professional services firm. Kroll began providing identity theft solutions in 1999 and created its Fraud Solutions practice in 2002 in response to increasing requests from clients for counsel and services associated with the loss of sensitive personal information, and related identity protection and restoration issues facing organizations and individuals. Since then, Kroll's Fraud Solutions clients have included Fortune 500 companies, non-profit organizations, and government entities dealing with healthcare, financial services, insurance, consumer service, and any activity involving the collection and use of personal information. Kroll's Fraud Solutions team presently serves over 10,000 businesses and millions of individual consumers. For more information, visit: [www.krollfraudsolutions.com](http://www.krollfraudsolutions.com).

**Confidential.** This material is CONFIDENTIAL to Kroll's Background Screening Division and Fraud Solutions Practice and may not be reproduced, published, or disclosed to others without the advance written authorization of Kroll.