

INVESTIGATOR INSIGHT

Identity Management – Top 10 Consumer Tips

ID Theft Awareness and Avoidance: Top Ten Consumer Tips

Identity theft is often described as one of America’s fastest-growing crimes. In today’s fast-paced world, sensitive information like names, Social Security numbers, and dates of birth are precious commodities. Here, we offer some simple actions and tools that consumers can utilize to reduce access to their sensitive information and improve the safeguards around it.

- 1. Think before you share.** Regardless of where you are when asked for your personally identifiable information (PII), think before sharing anything. Understand that, just because a field exists on an online profile page or a retailer’s preferred customer card application, you do not have to complete it. Along those same lines, it is important to show restraint when volunteering information about yourself in posts on social networking sites.
- 2. Keep security features updated on computers and other devices.** Use the security features designed to protect unauthorized access to your computer, phone, or other device. Then, keep the security software up-to-date, and run scans to look for malware that could hijack the device or allow your personal data to be captured. Also, be particular about what information you store on portable devices. When possible, store sensitive data on a secured network rather than on the device itself.
- 3. Don’t ignore the risk of “old-fashioned” types of theft.** Stealing physical items is still a popular method of obtaining PII. Don’t leave items that contain PII—purses, laptops, etc.—unsecured in your car, and keep these items close to you while out in public. Cross-shred documents containing personal information before discarding, and securely store any paper documents you intend to keep.
- 4. Watch for “shoulder surfers” and “skimmers.”** When using your credit or debit card in public, shield the entry of personal identification numbers (PINs), and be aware of people standing too close. With the advent of cell phone cameras, a shoulder-surfing thief can get your private information fairly easily.
- 5. Destroy or erase before you discard or donate.** If you recycle, toss, or donate your old electronic device, make sure you aren’t also giving away your data. Using

When asked for your personally identifiable information (PII), think before sharing anything.

A service of the Investigators of Kroll Fraud Solutions

These materials are derived from the research and discovery activities of Kroll Fraud Solutions’ Fraud Specialists and Licensed Investigators, and have been gathered from personal, historical, and aggregated experience performing specialized restoration services on behalf of Identity Theft victims. While believed to be accurate, these materials do not constitute legal advice, and are not guaranteed to be correct, complete or up-to-date. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll Fraud Solutions. These materials are provided for informational purposes only.

Identity Management – Top 10 Consumer Tips

the delete command just enables the computer to write over that space again; it doesn't actually eliminate the original bits and bytes. Some programs use a multi-pass wipe system to wipe data away that is better than a simple delete. However, physical destruction of the device or a component such as a hard drive may be the best way to ensure you're not tossing out or passing along your personal details.

- Understand that privacy is not the default setting on the web.** Explore security settings and privacy policies of websites before you use them. Default settings on social networking sites quite frequently allow any other users to access your data. Implement the security features available to you to restrict who has access to the information you share on the site.
- Avoid “ishing” scams.** A favorite tactic of fraudsters is to pretend to be someone that they are not in order to trick someone else into giving up PII. They represent themselves as a legitimate, often well-known business and ask for account numbers, Social Security numbers, or other data. Each method of contacting the potential victim has its own clever name that ends in “i-s-h-i-n-g.” Phishing is an attempt made via email. Fax phishing occurs via facsimile machine. Vishing uses telephone voice messaging systems. Smishing occurs via SMS (short messaging service), or text messaging. Before responding to a request for information, contact the company using a phone number you've found on your billing statement or their website to independently verify their need to reach you.
- Don't rely on fraud alerts or credit freezes alone.** Fraud alerts are meant to stop an identity thief from opening new accounts in your name. Credit freezes let you restrict access to your credit report, which would also make it hard for someone else to open new accounts. But, neither one will stop a thief from trading your PII for cash or using it for tax fraud, criminal identity theft, or any of the countless other ways fraudsters exploit stolen identities.
- Inventory your wallet's contents.** Make photocopies of any items containing personal information (both front and back, if applicable) in your wallet/purse: driver's license, credit cards, insurance cards, etc. Store these copies in a secure location. 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. If you find your Social Security card among the items in your wallet, remove it, and store it in a safe place. Carry it only on the day you know you will need it.
- Don't ignore warning signs.** Receipt of collection letters, unexpected bills, explanation of benefits statements listing medical services you didn't receive, or a credit report with inaccurate data are obvious signs that there might be a problem. Act on these items to determine the situation—whether or not the item is related to an error, something legitimate, or identity theft—and do so sooner rather than later.

Understand that privacy is not the default setting on the web. Explore security settings and privacy policies of websites before you use them.

A service of the Investigators of Kroll Fraud Solutions

These materials are derived from the research and discovery activities of Kroll Fraud Solutions' Fraud Specialists and Licensed Investigators, and have been gathered from personal, historical, and aggregated experience performing specialized restoration services on behalf of Identity Theft victims. While believed to be accurate, these materials do not constitute legal advice, and are not guaranteed to be correct, complete or up-to-date. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll Fraud Solutions. These materials are provided for informational purposes only.