Intersections Inc. Offers Consumers Seven Steps to Protect their Identities

Javelin Strategy and Research released the results of its 2010 Identity Fraud Survey Report. As a sponsor of this year's survey, Intersections Inc. offers the following seven steps to help protect consumers against identity theft:

- **Protect your computer** by installing up-to-date anti-virus and anti-spyware protection; use a firewall when you browse the Internet; and encrypt and safeguard portable devices and documents. Consumers need to be proactive and protect their computers with Intersections' IDENTITY GUARD® TOTAL PROTECTION℠ package which features an Internet Security Suite that provides proven anti-virus, anti-spyware, and firewall software that keeps computers safe from viruses, spyware, Trojan horses, worms, bots, and other malicious threats.
- **Protect your personal information from fraudsters** by opting for electronic delivery of your financial statements and other bills and shredding paper documents with personal information before disposing them. If you have important files—tax documents, medical records, bank account information—store them on a removable disc or external hard drive. Last year, according to Javelin's study, at least 13 percent of all identity crimes were committed by someone previously known to the victim. Intersections' IDENTITY GUARD TOTAL PROTECTION offers an on-the-go tool that provides secure storage and access to one's personal, financial, and medical information via any Web-enabled cell phone, PDA, or PC.
- **Protect your passwords and keep them out of sight at all times.** Never share your passwords with anyone; avoid using easy-to-guess common words or your personal information; change your password every 90 days; and use a unique password for each online account you create. Intersections' IDENTITY GUARD TOTAL PROTECTION includes ID VAULT™, giving consumers personal password protection that helps prevent online finances from falling victim to identity theft and fraud schemes by securely storing passwords so consumers can feel safe when they bank, shop, invest, or anything else that requires a password online. The PRIVACYPROTECT® feature adds another layer of protection by encrypting users' keystrokes to prevent identity thieves from stealing personal information and passwords as they are being typed on a keyboard.
- **Avoid fraudulent websites and only use legitimate sources** to contact financial institutions, such as an official website or the telephone number listed on statements and on the back of bank or credit cards. If you do visit one of these web sites, IDENTITY GUARD TOTAL PROTECTION will let you know if the site is legitimate and help you avoid making a risky decision. The ID Vault™ feature utilizes a white list of more than 9,000 financial and shopping sites that are continuously validated to make sure that users are not phished, pharmed, or redirected.
- **Don't Click on that Link!** Be wary of emails, phone calls, or text messages that may look as though they come from a legitimate company like your bank or the IRS, asking you to click on a link to update your personal information. This is called phishing, a technique used by identity thieves to steal your personal information. Scammers are increasingly using sophisticated technology such as "caller ID spoofing," which allows their number to appear as a legitimate business. Always verify that the sender of the message is legitimate! Do not return calls or text back with your personal information.
- **Protect your information on social networking sites** and restrict who can access your pages using built-in privacy settings. The Javelin survey found that fraudulent new e-commerce accounts, such as eBay and Amazon, and email payment accounts like PayPal, increased by 12 percent, indicating that fraudsters are targeting online Internet accounts. It's important to reveal as little as possible about yourself online, and always avoid revealing the type of information an identity thief wants such as family names, pet names, travel plans, your home address, school, employers, etc.
- **Invest in automated, identity theft monitoring tools.** The Javelin survey report shows that when consumers wait to find fraud on paper statements, they incur a higher out-of-pocket cost to recover and takes longer to detect — $274 and 39 days vs. $116 and 30 days — which is why expanding coverage to include comprehensive online monitoring is critical. To further minimize the impacts of fraud, consumers should start using some form of credit and online monitoring and Internet surveillance to make sure personal information like Social Security numbers, credit cards, and bank accounts are not being compromised.

For the best protection available, consumers should consider an identity theft monitoring service that provides more thorough and extensive protection than they can achieve on their own. Intersections' IDENTITY GUARD TOTAL PROTECTION is the most comprehensive offering on the market today covering personal information, credit scores, public records, computer, Internet, and mobile transactions. The service also provides sophisticated software that protects consumers against keylogging attacks, secures their passwords and user IDs as they navigate online, identifies legitimate websites, and protects their computers from advanced malware software. IDENTITY GUARD TOTAL PROTECTION also provides identity theft recovery services and financial reimbursement insurance in the event identity theft occurs.