

NEW PRIVACY AND IDENTITY THEFT LAWS NOW ON THE BOOKS

As stories about identity theft and privacy issues continue to dominate headlines, Attorney General Rob McKenna is working to educate Washington residents, businesses and law enforcement about new legislation that aims to prevent identity theft and protect consumers.

Several new state laws take effect next week that address security breaches, access to credit reports, and internet scams such as “phishing.”

“Identity theft and the resulting financial fraud are the fastest-growing crimes in the nation and here in Washington,” McKenna said. “I hear a new report almost daily about the havoc that cons have wreaked on families and businesses. These crimes cost U.S. consumers more than \$53 billion a year, and are some of the toughest to investigate and resolve.”

“Washington is at the forefront of dealing with privacy concerns and identity theft,” he continued. “Last session, the State Legislature passed several important laws that make it harder for identity thieves to operate in our state and easier for consumers to protect their personal information.

“These laws are a good foundation for addressing complex issues, but no one agency or business can prevent all fraud. The Attorney General’s Office is committed to helping stop identity theft before it happens by educating consumers. We are also a resource for local prosecutors who bring these criminals to justice.”

The following laws go into effect on July 24, 2006:

SECURITY BREACHES: Senate Bill 6043 requires agencies and businesses that own and license digital data to provide prompt notification in the event of a security breach in which personal information is compromised. The law is the Legislature’s answer to the ChoicePoint security breach, in which thieves posing as legitimate businesses were able to get access to personal information on nearly 145,000 consumers, more than 3,000 of them from Washington. At the time the theft was detected, California was the only state that required companies to notify consumers of such incidents.

CREDIT REPORT SECURITY FREEZE: Senate Bill 5418 allows identity theft victims to place a security freeze on a credit report, thereby prohibiting credit bureaus from releasing information without permission. The victim must first file a police report, and then send a request by certified mail to a credit bureau. Identity thieves often will try to open new credit accounts in a victim’s name, and merely placing an ‘alert’ on one’s account does not block new credit cards from being issued as a freeze would.

COMPUTER SPYWARE: House Bill 1012 cracks down on spyware that surreptitiously monitors a computer user’s actions. The law makes it illegal for anyone to transmit software to another computer without the owner’s knowledge, or to falsely entice someone to download software. It prohibits an unauthorized person from installing software that would take control of a consumer’s computer, modify its security settings, collect the user’s personal identification information, interfere with its own removal, or otherwise deceive the authorized user.

Violators can be fined actual damages or up to \$100,000, whichever is greater. The court may increase those damages by threefold for repeat offenders, up to a maximum of \$2 million. Washington is one of the first states in the nation to pass legislation to help stop this widespread consumer problem.

PROHIBITING “PHISHING”: House Bill 1888 amends the state’s spam statute to specifically prohibit “phishing” scams, in which identity thieves try to trick consumers out of personal information by sending emails that appear to come from a business, such as a bank or online auction site. The law makes it illegal for a person to misrepresent his or her identity in order to solicit personal information online.

Businesses affected by such fraud can bring a civil action in Superior Court to seek up to \$5,000 or actual damages. An individual may recover up to \$500 or actual damages, whichever is greater. Courts may increase the damages up to three times for repeat offenders.

DISCLOSURE OF PERSONAL WIRELESS NUMBERS: House Bill 1185 requires a wireless telephone company to obtain a subscriber’s express, opt-in consent in writing or electronically before publishing a wireless phone number in a directory. Subscribers can’t be charged for opting not to be listed.

Phone companies can be fined up to \$50,000 for each violation. In addition, an individual may bring a civil action to seek up to \$500 damages. This law is intended to protect consumers’ privacy and reduce the chance that they will be charged for calls made by telemarketers.

However, the law does not prohibit telemarketers from making unsolicited calls to wireless phones. Consumers can prevent calls from telemarketers by listing their home and wireless phone numbers in the FTC’s Do-Not-Call Registry. Register online at www.donotcall.gov or by phone at 1-888-382-1222.

POLICE REPORTS FROM ID THEFT VICTIMS: Senate Bill 5939 amends Washington’s identity theft statute to require police and sheriff’s departments to take reports from identity theft victims. The law does not require a law enforcement agency to investigate each report. Identity theft victims are required to file police reports in order to seek certain protections such as a credit freeze.

Reprinted from the Puget Sound’s *Update*, November 2005
and the SCAOA *Rental Gazette*, December 2005