

From the Desk of Attorney General Bob Cooper



May 20, 2010

AG Warns against On Line and Other Frauds

The capacity for thieves to steal your identity and commit fraud is only limited by their creativity. According to Tennessee Bureau of Investigation crime reports, online and other fraud is a serious problem in Tennessee. Federal Trade Commission statistics place our state in the top half of the nation in fraud, identity theft, and related consumer complaints. This means that all of us should remain vigilant against identity theft and other deceptive activity.

More people than ever are using the internet to shop, bank, search for jobs, and, as seen recently, donate to or volunteer for charitable work. While managing your life online is convenient, it may come at a high price if you are a victim of fraud or identity theft. But you can take steps to mitigate this risk.

The General Assembly has provided both my office and the District Attorneys powerful tools to use in combating identity theft and other fraud. Under consumer protection and criminal laws, identity theft is defined expansively, interpreted liberally, and subject to substantial financial and criminal penalties. Taken together, the laws protect a wide-range of sensitive information including biometric data, social security numbers, and health insurance account numbers from law breakers in this state. But unfortunately, many of the most sophisticated scams operate from beyond our state and national borders.

Consumers themselves are the front line defense against identity theft and related fraud. My office's Consumer Division works closely with the Commerce and Insurance Department's Division of Consumer Affairs to help Tennesseans learn how to avoid disclosing their personal information and to resolve those cases where sensitive data may have been compromised.

In some instances, it is not the consumer's fault that personal information is compromised. My office sees a number of cases in which personal information is compromised when the security of computer databases is breached at hospitals, schools, banks and other institutions, including government offices. All it takes in such cases is the theft of a single laptop, flash drive, or hard drive to provide access to extraordinary amounts of sensitive personal information.

In 2007, Tennessee and a group of other states led a multistate investigation into the theft of confidential information stored on computers owned by a major national retailer. Company officials said the hackers broke into an electronic system handling credit and debit card transactions as well as checks and merchandise returns for customers. Information from payment

cards and other transactions from almost 50 retail stores in Tennessee were potentially compromised. To resolve the case, the corporation voluntarily adopted heightened safeguards to protect sensitive customer information in the future.

The recent popularity of social media and the widespread use of internet “classified” advertisements to buy and sell furniture, cars and other personal items has created a new world of opportunity to pry into private lives and access private information. Hackers around the world surf the internet constantly looking for information they can collect and sell to others for fraudulent purposes. If you have a social media page, keep in mind that birthdays, family names, and even pet names can be valuable information for hackers searching for clues to passwords and other identity keys. When trying to rent an apartment or buy a vehicle, be very cautious about agreeing to provide credit reports containing sensitive information, and never wire money to someone you don’t know.

In addition to some of the more common scams, the Attorney General’s office receives many reports of attempted fraud and ID theft through email messages. For example, you may get an email from someone claiming you have won a contest or foreign lottery. But how can you possibly have won anything if you didn’t play or enter? Almost all of the online scams originate from an unsolicited email. If you don’t know someone who has emailed you, don’t respond and don’t open an attachment. Just delete it.

Finally, early detection is your best protection. Carefully review your credit card and debit card statements and other account information at least once a month. The longer it takes you to discover the fraud or identity theft, the longer it will require to secure your identity and recover lost funds. Take a few minutes to visit the website of the Tennessee Attorney General, where we have posted some additional tips and links to other websites with information on how to avoid identity theft and related fraud at: <http://www.tn.gov/attorneygeneral/>. If you have been a victim of identity theft, please contact the Division of Consumer Affairs by calling call 1-800-342-8385 or at <http://tn.gov/consumer/>.