TULLY RINCKEY PLLC
YOUR LAWYERS FOR LIFE - 1888LAW4LIFE.COM

Thomas Carr, Esq. discusses identity theft protection with the Albany Times Union

Identity thieves want your data
Take steps to protect yourself from identity thieves looking to tap into your finances

By T.J. King
June 9, 2014

Stealing is nothing new. However, the approach thieves use has changed. No longer do crooks look to rob people of their belongings; instead they long to acquire something much more valuable: the person's identity.

The Department of Justice defines identity theft as a crime in which a person uses a victim's personal data as if it was their own. This can be done by stealing someone's mail or hacking into a personal computer to get their hands on Social Security, bank account or a credit card numbers.Cybercrime is a problem for corporations as well as individuals. In late February, eBay had a reported 145 million accounts attacked. Encrypted passwords, home addresses, phone numbers and dates of birth were swiped from the website. Fortunately, there does not seem to be any financial loss or danger to these particular victims.But that's not always the case.Last holiday season, a Target server was commandeered by hackers and programmed to store numbers from credit cards used during the crush of holiday shopping. The information stolen included nearly 50 million credit card numbers and almost 100 million addresses, phone numbers and other pieces of personal information. Victims took legal action against Target for compensation or, at least, restitution for the lapse in protection.Many credit card companies offer their own consumer protection

services, flagging atypical transactions and contacting the cardholder to see if they were legitimate purchases. Often, they'll put a hold on the card until they've checked with the cardholder to make sure the card number hasn't fallen into the wrong hands. But you can help protect yourself.The state Attorney General's Office has a multitude of tips to stop identity theft, such as a credit freeze. A credit freeze does not allow anyone any sort of access to their line of credit. So, if the thief applies for a loan or tries to purchase something via credit, the lender would not be allowed access to the consumer's credit, making the transaction impossible. The drawback is when the victim reacquires their identity, they will need to allow the credit time to "thaw" and gradually be allowed to access their own information.The FBI suggests keeping all your personal information separate.If you have a document you regularly keep with you, do not put every piece of personal information — like your name, address and Social Security number — on there. Also, don't save documents or fill out Web pages with all your personal information, unless you're sure it's secure.To go along with prudent use of your computer, the FBI also advises that computers be equipped with firewalls and/or anti-virus software.Also, people should monitor their finances, says Thomas Carr, an attorney at Tully Rinckey in Albany."People should take advantage of the free online credit score options," Carr says. "I suggest that they space them out, doing one roughly every four months or so. This allows them to keep track of whether or not anything is wrong or out of the ordinary. If there is any discrepancy, they should report the problem immediately."The three companies that monitor credit are Experian, Equifax and TransUnion. Everyone is entitled to one free credit score per company per year. So, according to Carr, the wisest maneuver is to use each company's credit check individually. You can also log on to annualcreditreport.com or call (877) 322-8228 for your free report.Another way consumers can insulate themselves from identity theft is to be more realistic with their money."By lowering the spending limit on one's credit card, you are only giving potential hackers an allotted amount of your money, as opposed to all of it," Carr says."There are also credit monitoring companies whom people can pay to keep track of their credit, immediately getting in contact with them when a large or irregular purchase is made on a credit card."The sad truth, however, is no matter how careful you are, it's still possible to have your identity commandeered. When this happens, report

the breech to the fraud departments of the three credit monitoring companies immediately. Next up, contact the issuer of the account in question (ex: Mastercard) to close all affected accounts.After closing the accounts, call the police in the municipality where the fraudulent activity occurred. Victims should be sure to collect all police reports filed over the incident to have proof they were making strides to correct the problem.The victim should also keep a log of all suspicious activity.