INVESTIGATOR INSIGHT

Myth vs. Reality – Identity Theft

What you don't know can hurt you

When it comes to protecting Personal Identifying Information (PII) and reducing risk of identity theft, the more accurate information you have, the better off you are.

Here the Investigators of Kroll's Cyber Security & Information Assurance practice share some common myths about identity theft and the reality of each:

Myth: I use cash so I won't become a victim of identity theft.

Reality: There are two things to consider: First, just because you have not established a credit account, that doesn't mean somebody else will not use your PII to obtain credit. Second, identity theft affects far more than credit. Identity theft can involve criminal acts, medical care, banking, employment and more. It is important to monitor and protect your identifying information as much as possible regardless of your favorite payment method.

Myth: My credit report is monitored. I don't have to worry about identity theft.

Reality: Credit report monitoring can help you discover potential credit-related identity theft early. While it may then provide an opportunity to take steps to prevent other cases of credit-related identity theft, you must approach credit report monitoring as a valuable tool of detection rather than prevention. As stated in the previous myth/reality, a thief can use your PII to accomplish much more than opening new credit accounts.

Myth: Sensitive data can be transmitted safely via e-mail.

Reality: Unless you are encrypting your email message and sending the encryption key separately, email is not a safe way to share PII. Note that legitimate organizations will not ask you to share sensitive information via email.

Myth: You must supply your Social Security number (SSN) if asked for it.

Reality: The Social Security Administration explains on their website, that there are specific laws requiring a person to provide his or her SSN for certain purposes. Entities that request your SSN for legitimate purposes include, but are not limited to, the following: government tax and welfare agencies, financial institutions and securities brokerages, state moter vehicle departments and employers upon your acceptance of their offer of employment. Other entities may ask for it, because it is a readily available identifier. Before sharing this piece of sensitive data, ask why it is needed and if there is a different identifier you can give instead of your SSN. Memorize your SSN and do not carry your Social Security card with you routinely.

Myth: Paper records (or other physical documentation) with PII are much safer than electronic records.

Reality: Stealing physical items is still a very common method of obtaining PII. Items stolen may include a laptop computer, purse/wallet, files from an office, or even trash from a home or business. Secure items holding PII to the best of your ability and shred any papers containing PII before discarding.

Myth: Contacting a credit bureau is the best way to get a free credit report.

Reality: The Annual Credit Report Request Service was established in response to the FACT Act which mandates that consumers be given the opportunity to receive a free copy of their credit report from each national credit reporting agency one time every 12 months. You may request the free reports by contacting the Annual Credit Report Request Service through their website—www.annualcreditreport.com or by phone at 877-322-8228.

Myth: It is safe to respond to an unsolicited phone call or internet form as long as you recognize the name of the company.

Reality: Because of tricks such as domain masking and caller id spoofing, it is not safe to give sensitive information by phone or internet form unless you initiated the activity and are certain of the legitimacy of the entity with which you are dealing. If you receive a suspicious phone call or email, contact the entity that appears to have sent the communication using a phone number you obtain on your own and ask about the legitimacy of the communication you received.