



ID THEFT PREVENTION

by Texas Attorney General Greg Abbott

ACCORDING TO A RECENT FEDERAL REPORT, Texas is among the top states for identity theft. In the Federal Trade Commission's most recent Consumer Sentinel Network report, Texas ranks seventh in the nation for the most reported cases of identity theft per 100,000 residents. The FTC's report indicates that in 2012, there were more than 28,000 reported cases of identity theft in Texas.

According to the FTC, Texans lost a staggering \$77 million to identity thieves, fraud and other related complaints in 2012 – making Texas third in the nation for consumer losses in this arena. The Austin, Round Rock and San Marcos metropolitan area – one of the most wired areas in the nation – led the way as the metropolitan area in Texas with the most identity theft, fraud and related consumer complaints on a per capita basis.

Professional identity thieves are relying upon increasingly sophisticated tactics to support their burgeoning criminal enterprise. In one recently uncovered scam, for example, identity thieves attempted to steal senior Texans' sensitive personal information by posing as Medicare officials.

Falsely claiming to be affiliated with the federal Medicare program, identity thieves are contacting Texas seniors at home. The callers claim that the Medicare program's current identification cards – which are well known for the red, white and blue stripes across the top – are being phased out and that replacement Medicare cards must

be obtained in order for seniors to continue receiving benefits.

To obtain the new Medicare card, seniors are told they must confirm their Medicare number and bank account number over the phone. Since a senior's Medicare number is identical to his or her Social Security number, the caller's request to "confirm" a Medicare number is nothing more than a thinly veiled attempt to steal the unsuspecting senior's sensitive personal information.

Fortunately, a few wary seniors recognized the threat and questioned the would-be identity thief's intentions. But increasingly savvy identity thieves are prepared and attempt to create the false impression that they already have the senior's personal information. As proof, the callers often repeat some of the call recipient's personal information such as name, address and telephone number. But because this information is easy to obtain, the caller's verification effort is actually just a devious ruse that attempts to mimic the practices of legitimate enterprises – like a bank or insurance company – in an effort to steal the call recipient's Social Security and bank account number.

When personally identifying information – including Social Security and bank account numbers – falls into the wrong hands, Texans may suffer credit and damage – and even incur debts that were falsely racked up in their names. Identity thieves may use an individual's personal information to open new credit card accounts or commit

other financial crimes. When the identity thief fails to pay the bills on the accounts created in the victim's name, the delinquent accounts show up on the ID theft victim's credit report. Inaccurate credit history, if left uncorrected, may affect an ID theft victim's ability to get credit, insurance or even a job.

Every Texan should protect their personal information and never disclose sensitive information over an unsolicited phone call or at-home visit. Efforts to collect Texans' personal information should always signal a red flag. Another wise step Texans can take to protect themselves from identity theft is to shred or otherwise properly discard financial statements and other sensitive documents.

Texans who believe an identity theft scam may have affected them should access the Attorney General's Identity Theft Victim's Kit online at www.texasfightsidtheft.gov. The kit is designed to help victims navigate the process of protecting their credit. It includes relevant forms and agency contact information that is necessary to help restore credit and prevent further financial harm.

Whether they use email, telephone calls or even face-to-face visits, con artists dangle baited hooks in front of honest Texans every day. By recognizing the warning signs of an identity theft scam and sharing prevention tips with family and neighbors, Texans can help strengthen their communities and stop identity thieves in their tracks.

– May 2013

POINTS TO REMEMBER



IDENTITY THEFT SCAMS

Tips to avoid falling for the recent Medicare impersonation identity theft scam:

Never provide Social Security numbers, credit card numbers or bank account information to anyone who requests it during an unsolicited phone call or in-home visit.

If someone calls claiming to be affiliated with the federal Medicare program and demands Medicare numbers or other sensitive personal information, call recipients should hang up the phone.

Keep in mind that major federal agencies like the Internal Revenue Service and Medicare program never call Americans offering to provide services. These agencies communicate by U.S. mail – and never have their employees randomly call to confirm anyone's personal information.

To obtain a free credit report:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
(877) 322-8228
www.annualcreditreport.com

To learn more about how to avoid common identity theft scams, contact the Office of the Attorney General at (800) 252-8011 or visit www.texasattorneygeneral.gov.



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT