# HOW TO PROTECT SENSITIVE DATA AFTER A SECURITY BREACH

*by* Texas Attorney General Greg Abbott

SINCE APRIL, several breaches of security involving theft of electronic data and loss of property, including missing laptops and stolen memory drives, at public and private institutions have been announced. This recent string of security lapses may have compromised the sensitive financial and health information of millions of consumers and employees.

As you know, identifying information including names, Social Security numbers, and Driver's License numbers can lead to ruined credit and huge, undeserved debts when it falls into the wrong hands. An identity thief may use your information to obtain new credit cards, open checking accounts, get a bogus driver's license or Social Security card, make long distance calls, apply for a job, or make purchases using your bank account or credit card.

If you believe a security breach of personal information may have affected you, access the Attorney General's new **Identity Theft Victim's Kit** on our website at **www.oag.state.tx.us**. The kit is designed to help begin the process of recovering, both financially and legally. It includes relevant forms and agency contact information to help restore credit and prevent further victimization.

Carefully monitor bank statements, credit card statements and any other statements relating to recent financial transactions. Request a copy of your credit reports and examine them carefully for signs of fraud, such as credit accounts that are not yours. Check if there are numerous inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Also, check that your Social Security Number, address(es), phone number(s), and employment information are correct.

If you notice unusual activity on the statements, contact the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion – and request a fraud alert. When you request a fraud alert from one bureau, it will notify the other two for you. Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. Under the Fair Credit Reporting Act (FCRA), you can place an initial fraud alert for only 90 days. You may cancel the fraud alerts at any time.

When you establish the fraud alert, you will receive a follow-up letter from each credit bureau. Each letter explains how you can order a free copy of your credit report from that credit bureau. We suggest that you take advantage of this offer and order your credit reports soon. If you are a victim of identity theft, you will see evidence of it on your credit report.

You may also consider a security freeze. Texas law enables individuals to place a security freeze on their credit reports if they have filed an identity theft criminal complaint with law enforcement. A security freeze is stronger than a fraud alert because it prevents anyone from accessing your credit file until and unless you authorize the credit bureaus to release your report. (Please note that it does not affect existing accounts and includes other exceptions). Be aware that this might be inconvenient if you will be applying for new credit, an apartment, or employment involving a background check, since you will have to lift the freeze on your credit file. You can write to request that it be lifted for a certain period of time, or for a specific creditor.

If your credit report indicates you are a victim of identity theft, you will want to immediately file a police report. It is very important to do as you will use the report as proof that you are a victim of identity theft.

Report fraudulent accounts and erroneous information in writing to the credit bureaus and the credit issuers following the instructions provided with the credit reports. You will more than likely be asked for a copy of your police report.

In all communications with the credit bureaus, you will want to refer to the unique identification number assigned to your credit report and mail items certified, with return receipt requested. Be sure to save all credit reports as part of your fraud documentation.

The U.S. Department of Justice (DOJ) has the authority to prosecute identity theft at the federal level. You can report ID theft to federal authorities and receive additional assistance with identity theft-related issues through the Federal Trade Commission by calling 1-877-IDTHEFT (1-877-438-4338), or visit their Web site at www.ftc.gov.

## POINTS TO REMEMBER

### WHEN YOU SUSPECT IDENTITY THEFT

The Texas Attorney General's new **Identity Theft Victim's Kit is available at www.oag.state.tx.us.** If you suspect a security breach of confidential information may have affected you:

- Request a copy of your credit report and review it for unauthorized account activity.
- Report unauthorized charges and accounts to the appropriate credit issuers and credit bureaus immediately by phone and in writing. Cancel the accounts.
- File a police report with your local law enforcement agency and keep a copy of that report. Many banks and credit agencies require such a report before they will acknowledge that a theft has occurred.
- Contact the three primary credit reporting bureaus to have a security alert or freeze placed on your report:

**EQUIFAX FRAUD DEPARTMENT**
Phone: (888) 766-0008
Web: **www.equifax.com**

**EXPERIAN FRAUD DEPARTMENT**
Phone: (888) EXPERIAN (888-397-3742)
Web: **www.experian.com/fraud**

**TRANS UNION FRAUD DEPARTMENT**
Phone: (800) 680-7289
Web: **www.transunion.com**

ATTORNEY GENERAL OF TEXAS
GREG ABBOTT