



Strasburger
ATTORNEYS AT LAW

Business & Law Newsletter

BUSINESS & LAW NEWSLETTER • June 29, 2007 • [STRASBURGER & PRICE, LLP](#)

PREPARED BY



Marc F. Kirkland

2801 Network Boulevard,
Suite 600
Frisco, Texas 75034
469.287.3946 Direct

[marc.kirkland@
strasburger.com](mailto:marc.kirkland@strasburger.com)

EDITORS

Paul Myers

Billy Leonard

Business & Law Contacts

Jim Cameron

Buddy Ferguson

 [Printer friendly page](#)

 [View as Acrobat PDF](#)

 [Subscribe: RSS Feed](#)

SHRED IT OR DREAD IT

If your business is not in compliance with various Texas Anti-Identity Theft statutes, you might receive an unwanted visit from the Attorney General. Since identity theft has become one of the fastest growing crimes, both Federal and state authorities are devoting more resources to combat and prevent identity theft. As evidenced by recent lawsuits against Texas businesses, Texas Attorney General Gregg Abbott has been aggressively pursuing violations of Texas laws designed to prevent identity theft.

Every business operating in Texas should be aware of the 2005 Identity Theft Enforcement and Protection Act ("ITEPA") and Chapter 35 of the Business and Commerce Code ("Chapter 35") each of which contain penalties for failing to properly handle certain personal information. Both laws require that an individual's sensitive personal information be protected and safeguarded with reasonable procedures to prevent unlawful disclosure and that the records containing that information be destroyed by shredding, erasing or making the record undecipherable. Failure to comply with these provisions can expose your business to penalties of \$500 - \$50,000 per violation. Additionally, a violation of these statutes might also result in a violation of the Texas Deceptive Trade Practices Act.

As Radio Shack, CVS, and other businesses who have been targeted by the Attorney General are aware, violations of these laws can result in large fines. However, that is not all. A business may also receive negative press, lose employees and customers, and be sued by employees and customers whose personal information has been compromised. The following are some steps your business can take to protect itself from exposure to enforcement.

Know and Understand What the Law Requires for Handling and Disposing of Personal Information

In order to protect your company, know where originals and copies of business records containing personal information - whether in paper or electronic form - are maintained and how they are disposed. You will probably learn something you did not know about your company and its data. The types of records which must be protected under

these statutes include original or reproductions of handwritten, typed, or electronically stored documents or data that contain an individual's name, social security number, driver's license number, debit or credit card number or other personal information.

Second, determine whether your company's processes for destroying these records comply with Texas law. The law requires that after the applicable retention period, business records are to be destroyed by shredding, erasing or making the personal information undecipherable.

Third, determine if your company's processes are in writing and contained in a document/data retention and disposal policy. While not specifically required by the law, having written instructions that outline your company's legally compliant retention and disposal policies will increase awareness among your employees and help ensure full compliance.

Ensure Legal Compliance Procedures are in Place to Deal with Security Lapses

Analyze and determine if your company has in place procedures for dealing with a security lapse that may disclose your customers' personal information to identity thieves. For instance, ITEPA has specific notification requirements that must be employed if a breach occurs. If there is a breach, your company must move "as quickly as possible" to notify (a) each Texas resident whose information was disclosed without authorization, (b) the owner or license holder of the data, and (c) if more than ten thousand individuals were exposed in the breach, then all consumer reporting agencies.

Many of the steps required by these laws take a common sense approach to handling and destroying business records that contain personal information. That being said, the recent push by the Attorney General's office has identified a number of large national companies that have exposed their customer's confidential information and, consequently, may be subjected to massive fines and the potential for costly litigation. In this time of increased focus on identity theft and the security of personal information, it may be time for your business to revisit its procedures for handling its employees and customers' personal information.

PUBLICATIONS:

- To view past issues of the Business & Law Newsletter, please visit [Business & Law Newsletter](#)
- To subscribe to other Strasburger publications, please visit [Strasburger Publications](#)

DISCLAIMER: Articles contained within this newsletter provide information on general legal issues and are not intended to provide advice on any specific legal matter or factual situation. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel.

ADVERTISEMENT NOTICE: This e-mail may constitute a commercial electronic mail message subject to the CAN-SPAM Act of 2003. If you do not wish to receive further commercial electronic mail messages from the sender, please send an e-mail to Strasburger@Strasburger.com and request that your e-mail address be removed from future mailings. To update your address, please send an email to Strasburger@Strasburger.com including the updated information. Strasburger & Price, LLP, 901 Main Street, Suite 4400, Dallas, TX 75202.

