October 2010

MAKING YOUR INTERESTS OUR BUSINESS.™

FRIEDMAN & FEIGER
ATTORNEYS AT LAW

BANKRUPTCY + BUSINESS LAW + COMMERCIAL LITIGATION + CONSTRUCTION +CORPORATE +ENTERTAINMENT LAW + FAMILY LAW + HEALTHCARE +HOTEL & HOSPITALITY LAW
INTELLECTUAL PROPERTY + LABOR AND EMPLOYMENT + PERSONAL INJURY + PRODUCTS LIABILITY + REAL ESTATE + SECURITIES + TAX + TRANSPORTATION + TRUSTS & ESTATES

PASSWORD SECURITY
(If I tell you my Password, I'll have to kill you!)

Passwords are a critical part of your electronic identity and network security. Passwords serve to protect user accounts and help to determine accountability for all transactions and other changes made to system resources, including data. Your password gives you access to a variety of computing services on your network depending on the capabilities of the individual computer or system you are using.

Every time you connect, you must provide your password; you must prove who you say you are. If someone else guesses or steals your password, he or she can access all of the information tied to that password. If you share your password with a colleague or friend, you are giving an unauthorized individual access to the system and you will be held responsible for their actions. This includes access to your files, your e-mail, your funds, your personal information and more, depending on what the password was supposed to protect. For example, having the password to your online bank account may allow someone to bill items to your credit card, transfer money from your account, or pay their own bills with your money. If the individual gives your password to someone else, if some of your files are deleted or otherwise rendered unusable, if an unauthorized individual uses your access privileges to damage information on the system, or makes unauthorized changes to data, you could cause serious damages and expose yourself to enormous liability. In short, an insecure password can easily wreak havoc in your life.

You will not be the only person affected by a stolen password. Other users on your network and on the Internet could potentially be affected as well. Once an intruder with the necessary knowledge, experience, and tools gains entry to a system, he or she may be able to access and control other computers and systems on the same network and capture information about local users. If these users then connect to other networks, the intruder has the potential to penetrate and control the remote systems to which the local users connect, thereby increasing the likelihood of a breach in the security of those systems as well.

Unfortunately, today it does not even take a skilled intruder to control a computer on which he or she has an account. Many of the tools required to gain control over a computer can be downloaded from the Internet and used with little or no knowledge of how they work. These intruders may not have the knowledge necessary to break into a computer without help, but because of the availability of hacking tools and the large number of them, they can cause a great deal of trouble.

Authentication of individuals as valid users, via the input of a valid password, is required to access any number of shared computer information systems, including the network, e-mail, the Web, and voicemail. Each user is accountable for the selection, confidentiality and changing of passwords required for authentication purposes. Since most people are responsible for picking their own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardize information that they are supposed to protect; good ones do not. Poor or weak passwords are easily cracked, and put your entire system at risk. Therefore, strong passwords are essential.

The following are some tips to help you create strong passwords:

(Continued on page 2)

INSIDE

Password Security (continued)	2
Preserving E-Evidence for Litigation	3
So You Won A Judgment, Now What?	3
Wednesday's Child "Belonging" Luncheon	4
Calendar of Events	4

Password S-E-C-U-R-I-T-Y (continued)

(Continued from page 1)

DO change passwords frequently. Change your password every 90 days or whenever you sign in to a site you haven't visited in a long time. Don't reuse old passwords. Password managers should assign expiration dates to your passwords and remind you when the passwords are about to expire.

DO keep your passwords secret. Putting them into a file on your computer, e-mailing them to others, or writing them on a piece of paper in your desk is tantamount to giving them away. If you must allow someone else access to an account, create a temporary password just for them and then change it back immediately afterward.

DO create a password that contains at least 8 characters. Your passwords should contain at least 5 uppercase letters (e.g. "F") or 5 lowercase letters (e.g. "p") or a combination of both. Also, use at least 2 numerical characters (e.g. "5") and at least 1 special character (e.g. "$").

DON'T use passwords comprised of dictionary words, birthdays, family and pet names, addresses, or any other personal information. Don't use repeat characters such as **111** or sequences like **"abc"**, **"qwerty"**, or **"123"** in any part of your passwords.

DON'T use the same password for different sites. Otherwise, someone who culls your Facebook or Twitter password in a phishing exploit could, for example, access your bank account.

DON'T allow your computer to automatically sign in on boot-up and, thus, use any automatic e-mail, chat, or browser sign-in. Avoid using the same Windows sign-in password on two different computers.

DON'T use the "remember me" or automatic sign-in option available on many Web sites. Keep sign-ins under the control of your password manager instead.

DON'T enter passwords on a computer you don't control — such as a friend's computer — because you don't know what spyware or keyloggers might be on that computer.

DON'T access password-protected accounts over open Wi-Fi networks — or any other network you don't trust — unless the site is secured via **https.** Use a VPN if you travel a lot.

DON'T enter a password or even your account name in any Web page you access via an e-mail link. These are most likely phishing scams. Instead, enter the normal URL for that site directly into your browser, and proceed to the page in question from there.

DON'T use a password that is trivial, predictable, or obvious.

DON'T use a password that is based on publicly known fictional characters from books, films, t.v. and so on.

DON'T use a password that is based on your company's name or geographic location.

DON'T re-use old passwords for a period of at least 1 year.

If an employee either knows or suspects that his/her password has been compromised, it should be reported to the IT Department and the password changed immediately.

Effective passwords are passwords that are secure, user friendly and supportable within the confines of both technology and human behavior.

Disclaimer: The comments expressed herein are not claimed to be comprehensive, complete or necessarily correct in all circumstances. The comments expressed herein are general comments relating to individual user's accounts under ordinary circumstances. Anyone with special circumstances or anyone setting up special services should seek further legal advice from one of our attorneys.

Sincerely,

Larry Friedman

Larry Friedman can be reached at (972) 788-1400 or e-mail him at lfriedman@fflawoffice.com

Preserving E-Evidence for Litigation By Michael Donohue

In today's electronic information world, business owners are invariably faced with an obligation to preserve electronic data once a lawsuit is reasonably anticipated.

In Texas, the law imposes a general duty to preserve evidence once a party knows, or should reasonably know, that there is a substantial chance that a claim will be filed, and that evidence in the party's possession or control will be material and relevant to that claim. *Wal-Mart Stores, Inc. v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003). Once litigation is threatened, you should suspend normal destruction and archiving processes of any electronic data that is potentially relevant to the lawsuit -- i.e., e-evidence. Counsel for clients threatened with litigation should work with clients to ensure that "litigation hold" procedures are put into effect to preserve business data. The client should suspend its routine document/electronic data retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents and data. Counsel for potential plaintiffs may wish to enforce the duty to preserve evidence on the opposition, including the duty to preserve electronic data, by sending an "evidence preservation letter" to the opposing party.

A party's obligation to preserve electronic data does not end with the implementation of a "litigation hold", as once litigation begins, the preservation obligation is only the beginning. Once a lawsuit is filed the discovery process begins. Consequently, counsel for the client must not only oversee compliance with the litigation hold of relevant electronic data, but work with the client to retain and produce relevant electronic information and documents. It is important for litigation counsel involved in the discovery of electronic data to understand the basic structure of the storage and archival process of both the client and the opposing party. Among the questions to be considered for both producing and seeking production of e-evidence are (i) is there a backup policy?; (ii) to what extent is that backup policy followed?; (iii) do backups occur automatically or do they require manual input?; (iv) how long is archival data retained?; (v) is archived data easily accessible?; (vi) is there more than one backup system or server?; (vii) how good is the indexing of backed up data?; and, (viii) are backup tapes or logs available?

Remedies available to a party when an opposing party destroys or fails to preserve evidence, including relevant electronic data, are generally fashioned on a case by case basis at the discretion of the trial court. A trial court judge has discretion to fashion a remedy that will restore the parties to a rough approximation of the same positions they would have been absent the loss or destruction of evidence. *Wal-Mart Stores, Inc.*, 106 S.W.3d 721. Such remedies may include a spoliation of evidence instruction to the jury (i.e., an adverse inference instruction) and, in some cases, "death penalty" sanctions (e.g., striking of a party's pleadings).

From the time litigation is first anticipated, Friedman & Feiger's legal team will work with and assist you in preserving relevant electronic and business data, notify the opposing party of its duty to preserve evidence, and pursue discovery of the opposing party's relevant electronic data.

Mike Donohue can be reached at (972) 788-1400 or e-mail him at mdonohue@fflawoffice.com

So You Won a Judgment, Now What? By Ryan Lurich

Successful collection of a judgment requires aggressive use of the post-judgment remedies available to a judgment creditor. While there are numerous post-judgment remedies available to a judgment creditor, the ultimate decision on which, if any, to use should be based on a careful cost/benefit analysis. The best remedy of all may be to negotiate a post-judgment payment plan in exchange for the judgment creditor withholding further collection efforts.

The least expensive remedy, but probably the most important, is to have the judgment abstracted and filed in the county records. This simple act creates a judgment lien on all of the judgment debtor's non-exempt real property in the county of recordation. The judgment lien continues for a period of 10 years following the date of recordation, unless it becomes dormant, in which case the lien ceases to exist. In order to prevent a judgment lien from becoming dormant, a judgment creditor must request that a writ of execution be issued within 10 years of the date of judgment. Additionally, the judgment lien may be renewed for successive 10 year periods by requesting a writ of execution at least once in each 10 year period.

After a judgment has been entered in your favor, Texas law allows you to send the judgment debtor post-judgment discovery asking the judgment debtor to identify the existence of, and location of, his/her/its assets. Post-judgment discovery is a powerful tool because the Court can enforce a judgment debtor's failure to answer post-judgment discovery fully and truthfully through its contempt powers.

A writ of execution is a judicial document directing the sheriff or constable to enforce the judgment by levy, taking possession of the debtor's non-exempt property, and then selling it and delivering the proceeds to the judgment creditor.

Post-judgment garnishment is a procedure by which judgment creditors can inquire into the relationship between the judgment debtor and a third-party to determine if the third-party is holding any funds or property owing to the debtor. If the third-party does owe the debtor funds or property, the garnishment procedure directs the third-party to pay the funds to the judgment creditor rather than to the judgment debtor to satisfy the judgment.

Turnover is another powerful remedy available to a judgment creditor. The purpose of the turnover statute is to aid the diligent judgment creditor in obtaining satisfaction of the judgment by requiring the judgment debtor to turnover the debtor's property that cannot readily be attached or levied on by ordinary legal process. In a turnover proceeding, the judgment creditor identifies for the Court the property that the judgment debtor owns that cannot be attached or levied on by ordinary legal process (e.g., shares of stock ownership in a corporation) and the Court orders the judgment debtor to deliver that property to the sheriff or constable to sell and deliver the proceeds to the judgment debtor. A judgment debtor's failure to comply with a turnover order may be enforced through the Court's contempt powers.

Notwithstanding that Texas has very good laws protecting debtors, knowing your rights and what legal remedies are available to you will help you collect your money and prevent the hard fought judgment you won in Court from being a hollow victory.

Ryan Lurich can be reached at (972) 788-1400 or e-mail him at rlurich@fflawoffice.com

FRIEDMAN & FEIGER
ATTORNEYS AT LAW

5301 Spring Valley Road, Suite 200
Dallas, Texas 75254

Phone: 972-788-1400
Fax: 972-788-2667

PLEASE VISIT OUR AWARD WINNING WEBSITE!

WWW.FFLAWOFFICE.COM

WEDNESDAY'S CHILD "BELONGING" LUNCHEON
FRIDAY, DECEMBER 3RD AT THE RITZ CARLTON

Friedman & Feiger will bring opportunities to many deserving North Texas foster children as title sponsor of the Wednesday's Child "Belonging" Luncheon to be held at the Ritz Carlton on Friday, December 3rd. Janelle and Larry Friedman are co-chairpersons for the fund-raising luncheon.

Leigh Anne Tuohy will be the luncheon speaker. Leigh Anne Tuohy was featured in Michael Lewis' 2006 book, The Blind Side: Evolution of a Game, later made into a feature film, *The Blind Side*. In the film, Tuohy was portrayed by actress Sandra Bullock, who won an Academy Award for Best Actress for her performance.

Janelle and Larry Friedman will honor Myrna Schlegel for her heartfelt commitment and many years of helping foster children. Lance and Julie Brennan will be honored for "walking the walk" with the first annual '*Gloria*' Award. WFAA Channel 8's Gloria Campos will serve as the event's mistress of ceremonies.

The event will feature a silent auction of art featuring a heart donated by celebrities and famed local artists.

One out of every 207 children in North Texas is a foster child and the need for assistance is ever increasing. After being removed from their homes due to abuse or neglect, foster children often have to start their lives over in a new place at a young age. Wednesday's Child's mission is to assure each child's needs are met while in the foster care system and to give each child as normal a childhood as possible. If you would like to help, please contact Janelle Friedman at: jfriedman@fflawoffice.com

Upcoming Events

Friedman & Feiger Calendar

September 25, 2010	**Janelle Friedman receives the 2010 "Brilliantly You" Award from Women That Soar**
October 7, 2010	**Essential Energy Reception hosted by Neiman Marcus**
November 4, 2010	**Essential Energy Reception hosted by Janelle Friedman**
November 10, 2010	**Friedman & Feiger hosts Courthouse Appreciation Event**
December 3, 2010	**Janelle and Larry Friedman Co-Chair "Belonging" Luncheon benefiting Wednesday's Child at the Ritz Carlton**