



Tanner & Guin, LLC
COUNSELORS AT LAW

Capitol Park Center
2711 University Boulevard
(35401-1465)
P.O. Box 3206
Tuscaloosa, Alabama 35403-3206
Telephone: (205) 633-0200
Facsimile: (205) 633-0290

632 Gulf Shores Parkway,
Suite 208
P.O. Box 4328
632 Gulf Shores Parkway,
Suite 208
Gulf Shores, AL 36542
Telephone: (251) 968-0200
Facsimile: (251) 9680290

E-mail: info@tannerguin.com

Security and Privacy Law Practice Group

Blake A. Madison
(205) 633-0246
E-mail:
bmadison@tannerguin.com

Carol Armstrong
(205) 633-0268
E-mail:
carmstrong@tannerguin.com

Thomas W. Scroggins
(205) 633-0227
E-mail:
tscroggins@tannerguin.com

Inside this issue:

New Newsletter to Keep You Informed.....	1
<i>As the security and privacy of personal information becomes a larger and more expensive issue for businesses, this newsletter will serve to provide you with information on what is happening on the legal side of these issues.</i>	
How Much Will a Data Breach Cost Your Company?	1
<i>It seems there is a new data breach in the news each day. The question many companies must ask is how much will it cost them if they fail to take the necessary security precautions to avoid such a breach.</i>	
FTC Provides Practical Solutions for Businesses on Safeguarding Personal Information	2
<i>The Federal Trade Commission has published a common sense guide for businesses on the topic of protecting personal information.</i>	
Health Privacy Laws Can Work Against You	2
<i>While privacy laws passed over the past 10-15 years are designed to protect you, sometimes they can actually become a burden and work against you.</i>	
ChoicePoint Settles with 43 States After 2005 Identity Theft Incident.....	3
<i>The cost of ChoicePoint's well-documented security breach continues to rise.</i>	
Massachusetts Bill May Lead the Way to Punishing Businesses for Poor Data Security.....	3
<i>In a move that is likely to be closely followed, Massachusetts lawmakers are examining the possibility of transferring much of the cost of poor data security from bankers to the businesses that fail to secure their data.</i>	
U.S. Senate Considers Move Away from Real ID Act.....	4
<i>As a result of significant backlash across the country, the U.S. Senate is considering at least delaying some of the requirements of the Real ID Act of 2005.</i>	

New Newsletter to Keep You Informed

As the security and privacy of personal information becomes a larger and more expensive issue for businesses, this new newsletter from the attorneys of Tanner & Guin, LLC will serve to provide you with information on what is happening on the legal side of these issues on an approximately quarterly basis. If you wish to continue to receive this newsletter and the important information each issue will contain, please let

us know by filling out the response form at the end of this newsletter or by e-mailing your name, company, and e-mail address to Sheila Vaughn at receptionist@tannerguin.com. If we do not receive your request, we will assume you do not need information on security and privacy law issues and will cease sending these newsletters to you in the future.

How Much Will a Data Breach Cost Your Company?

Calculating the cost of a security breach is difficult at best, but one thing is for sure— data breaches are expensive. Companies must take into account not only direct costs of the breach, such as recovering and re-securing breached data, but also must assess the associated costs of the breach (i.e., restitution and legal costs generated from lawsuits initiated after the breach, lost employee productivity, potential regulatory fines, cost of notifying customers). On top of all of these costs, the breach will inevitably

create a loss in customer confidence that may be nearly incalculable.

So what is the bottom line? According to a new study from Forrester Research, Inc., the average security breach can cost a company between \$90 and \$305 *per lost record* depending on whether the company is low or high profile (the recent TJX breach is their idea of high profile). According to the research, companies can expect to spend around \$50 per record on discovery,

(Continued on page 2)

How Much Will a Data Breach Cost Your Company?

(Continued from page 1)

notification, and response issues. Lost employee productivity accounts for another \$20 per record. The remaining expenses come from opportunity costs from lost customers, regulatory fines, and other legal expenses.

For companies with at least 1000 records, Darwin Professional Underwriters, Inc. has created a Data Loss Cost Calculator to show the potential cost of a breach. Users input the number of breached records and immediately receive estimates for the total cost of a breach along with the costs for other breach related activities such as customer notification, media management, state fines,

and credit monitoring. To access the free online calculator, go to <http://www.tech-404.com/calculator.html>.

The estimates above are certainly not perfect and every breach will create new costs that are unique to each business, but estimates are helpful to determine a baseline cost associated with data incidents. These figures illustrate that the smartest and cheapest solution to a breach is obviously not to have one at all. Spending a little time and funding in prevention of and preparation for a breach could save your company thousands of dollars, if not more.

“...the smartest and cheapest solution to a breach is obviously not to have one at all.”

FTC Provides Practical Solutions for Businesses on Safeguarding Personal Information

The Federal Trade Commission now offers a common sense guide for businesses on the topic of protecting personal information. The short guide is divided into five broad principles and contains straightforward suggestions that do not require a technical background to understand. The five principles are: (1) Take Stock - Know what personal information you have in your files and on your computers; (2) Scale Down - Keep only what you need for your business;

(3) Lock It - Protect the information that you keep; (4) Pitch It - Properly dispose of what you no longer need; and (5) Plan Ahead - Create a plan to respond to security incidents. The guide not only provides information detailing how to secure information, but also offers tips on identifying risks, training employees, and acting wisely in the event of a breach. A copy of the brochure and more information can be found at www.ftc.gov/infosecurity.



Health Privacy Laws Can Work Against You

The Health Insurance Portability and Accountability Act (HIPAA) took effect in 1996 and ensures a national floor of privacy protection for patients and protects medical records and other individually identifiable health information by forcing health care companies to implement security features and employee protocols to protect information. Unfortunately, the precautions implemented to date are far from perfect. It is still all too common to learn that hospitals around the country have exposed sensitive patient data to the public, but in addition to the absence of protection provided by HIPAA, the act can work against individuals in several other ways.

health records, but a covered entity may deny a person the right to an amendment if the protected health record was not created by the provider or insurer currently using the information. Based on this rule, if one medical entity creates a medical record and sends the record to a second entity, the individual will have no way to force the second entity to correct the record. This creates the possibility of incorrect medical information being disseminated to multiple medical entities with little or no way to correct the multiple records.

Also, HIPAA sets out several instances where an individual may not be able to see his own records. Notably, if a healthcare

“HIPAA sets out several instances where an individual may not be able to see his own records.”

HIPAA gives an individual the right to review and seek amendment to his or her

(Continued on page 3)

Health Privacy Laws Can Work Against You

(Continued from page 2)

provider determines that records in an individual's file have been fraudulently replaced with records of another person, then that individual cannot see the records because they now consist of HIPAA protected information of another person.

Finally, it appears that HIPAA may be able to work against the general safety of society in some respects. State health officials in Virginia recently refused to answer questions from a governor appointed panel regarding Seung-Hui Cho's prior medical and mental health treatments. The panel is investigating Cho, the individual responsible for the April 16

shooting and killing of 32 at Virginia Tech, to attempt to determine why the killings occurred and prevent more incidents like that from happening. HIPAA regulations would have allowed some of Cho's medical records to be examined when he was alive because medically he was considered a danger to himself, but because HIPAA's protections continue indefinitely after the death of a person and Cho is no longer a threat, his records are protected.

If you have any questions regarding HIPAA or medical records privacy in general, please contact Blake Madison at bmadison@tannerguin.com or (205) 633-0246.



ChoicePoint Settles With 43 States After 2005 Identity Theft Incident

ChoicePoint, Inc. recently settled with 43 states regarding a massive identity theft incident in 2005. The breach involved thieves posing as small business customers and ended with the compromise of personal information of 163,000 people. ChoicePoint will pay no specific fine in the current settlement but the company agreed to pay \$500,000 to fund state public education campaigns about identity theft. This settlement came a year after

ChoicePoint agreed to pay \$15 million to the Federal Trade Commission because the company's security and record-handling procedures violated consumers' privacy rights. The \$10 million fine coupled with the \$5 million ChoicePoint paid to reimburse individuals is the largest fine collected by the Federal Trade Commission to date in a data security incident.

"This settlement came a year after ChoicePoint agreed to pay \$15 million to the Federal Trade Commission."

Massachusetts Bill May Lead the Way to Punishing Businesses for Poor Data Security

Massachusetts lawmakers may be on the forefront of placing liability from security breaches on businesses rather than on banks. Currently many of the customer expenses associated with security breaches such as canceling or reissuing credit cards, stopping payment, and refunding customers have been absorbed by the banks issuing the credit cards to the victims. The banks that allow businesses to accept credit card transactions are penalized by American Express, Visa, and other credit card companies if the businesses are found to be in violation of the Payment Card Industry's data security standards.

Massachusetts House Bill 213, sponsored by Representative Michael Costello (D), is the first of its kind and would force companies whose security systems are breached to assume full financial responsibility for the customer

related costs. The bill would apply to all companies doing business in Massachusetts regardless of where the company is based, but the types of fraud covered are limited. The bill only covers fraud where a specific company's security system is breached and does not cover other fraud, such as those resulting from stolen or lost cards.

Although this is a state measure, if the law passes, the impact could be felt nationwide due to the government and individuals demanding accountability in dealing with information security issues. Were Massachusetts to require companies to meet higher security standards coupled with heavy repercussions for failure to meet those standards, it is doubtful that other companies outside of the state will be allowed to scrape by without accountability for very long from other states.



U.S. Senate Considers Move Away from Real ID Act

During recent floor debate on a new immigration bill, Senators preserved an amendment that will forbid new identification cards from being mandatory to gain employment in the United States. The original immigration bill would require employers to demand a federal identification card as approved by the Real ID Act of 2005 before hiring any new employees after 2013. The amendment removes the requirement for identification to gain employment and prohibits the use of federal funds to create a system to check the identification.

The Real ID Act of 2005 will require Americans, starting in 2008, to have a federally approved identification card to travel on an airplane, to open a bank account, or to take advantage of nearly any government service such as social security. In addition to those requirements, the act also will require identification to gain employment in the

United States starting in 2013. The new ID cards, mandated by the federal government, will include a universal strip or a radio frequency identifying device containing much more information than the current driver's license and are seen by many as an encroachment of privacy.

The vote taken to preserve the amendment to the immigration bill was merely preliminary. If the new immigration act fails or passes without the amendment, the Real ID Act will remain unchanged. The Department of Homeland Security has defended the Real ID Act as a way to limit illegal immigrants and prevent terrorists from getting driver's licenses. On the other hand, a number of states have already enacted or are in the process of enacting legislation to block the Real ID Act and feel that the individual privacy concerns are highly important.

*The new ID
cards...are seen by
many as an
encroachment of
privacy."*



Blake Madison, a partner with the firm, is a Certified Information Privacy Professional and works closely with businesses in tackling security and privacy issues. Mr. Madison also practices in the areas of business, corporate and commercial law, with an emphasis on the health care industry. He has experience handling complex contract negotiations. Mr. Madison has additional experience in the areas of state and local taxation, industrial development issues, and real property issues.

Sign up for Security and Privacy Law Newsletter

To receive future editions of our new "Security and Privacy Law" newsletter, please fill out the information below and e-mail it to receptionist@tannerguin.com, or fax it to (205) 633-0290.

Name: _____ Company: _____

Title: _____ E-mail Address: _____

Copyright © 2007 Tanner & Guin, LLC All rights reserved.

This newsletter is intended for general information purposes only and should not be construed as providing legal advice or legal opinions on any specific fact situation. Readers are urged to consult their own legal advisors concerning any specific legal questions involving the issues discussed. Personal opinions of the authors are included. Comments and suggestions are solicited and should be forwarded to any member of our *Security and Privacy Law Practice Group*.

NOTE: The Alabama State Bar requires the following disclosure: "No representation is made that the quality of the legal services to be performed is greater than the quality of legal services performed by other lawyers." Mississippi State Bar requires: FREE BACKGROUND INFORMATION AVAILABLE UPON REQUEST.
