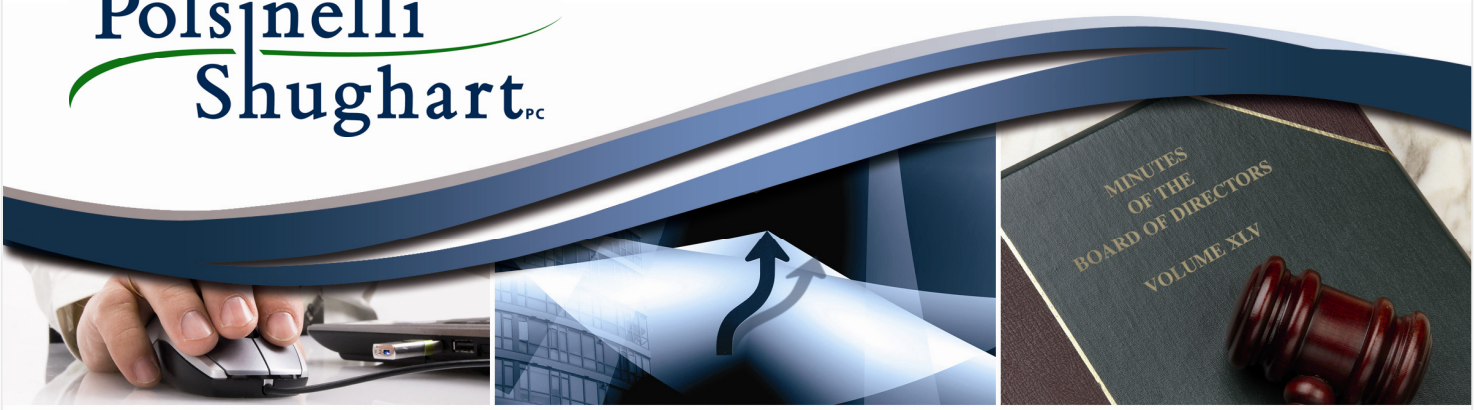
Polsinelli Shughart PC



Corporate Law | e-Alert

November 2009

Identity Theft and Data Privacy:
A Polsinelli Shughart Update

In this issue:

Recent legislative attempts to curb the growing scourge of identity theft may in fact impose additional costs and responsibilities on small business owners. Here's a look at three significant developments:

1. Red Flag Rules — Implementation of Regulations Delayed

This federal statute passed in October of 2007 requires those subject to the law to implement written identity theft prevention programs to detect, prevent and mitigate identity theft. Financial institutions generally were required to comply with the Red Flag Rules implemented in November of 2008, while others subject to the law were to comply at a later date. In addition to financial institutions, the statute applies to "creditors" defined as "any person or business who arranges for the extension, renewal or continuation of credit."

The proper scope of the Federal Trade Commission ("FTC") regulations implementing the statute has been the subject of much debate. While it has been relatively easy to agree that the statute was intended to apply to car dealers, utility companies and phone companies, the FTC's contention that it applies to any business (like a doctor's office or law firm) that does not require payment in full before rendering services, has been less well received. The enforcement date of the regulations has been delayed to **June 1, 2010**.

2. New Federal Rules for Health Information

The American Recovery and Reinvestment Act of 2009 ("ARRA"), commonly known as the "Stimulus Bill," contains some provisions not directly aimed at stimulating the U.S. economy. Two such provisions require certain holders of personal health information records and those subject to the Health Insurance Portability and Accountability Act ("HIPAA") to disclose when the security of individually identifiable health information is breached. Highlights of the new regulations (to be promulgated and enforced by the FTC in the case of personal health records and the Department of Health and Human Services in the case of HIPAA) include:

Personal Health Records – FTC

- An electronic record of health information with respect to an individual which identifies (or there is a reasonable basis to believe it identifies) the individual
- Applies to any vendor of a personal health record or a related entity and third-party service providers to these vendors
- Breach of security includes the acquisition of any unsecured identifiable health information of an individual without authorization of that individual
- Those vendors of Personal Health Records and PHR-related entities or their service providers must notify any individual whose information was acquired in the breach and notify the FTC
- The notification period begins on the first day of discovery of the breach or when it should reasonably have been known to such vendor

- Notice to the FTC and media is required when there is breach of security of 500 or more residents in the state or jurisdiction, and generally must be made no later than five (5) business days after the discovery of the breach. If the breach involves unsecured PHR of fewer than 500 individuals, the vendor may maintain a breach log and submit such log annually to the FTC

- The notification to individuals and the media, if necessary, must be made "without unreasonable delay" and in no case later than sixty (60) calendar days after discovery

- The proposed regulation sets out methods of notice, both when it is notice to the individual, to the FTC and to the media, and specific content for each of the forms of notices

HIPAA Entities — HHS

- HIPAA only applies to covered entities which are health plans, health care clearing houses, and health care professionals who maintain health information in electronic form and electronic transmission. The breach notification rules also apply to business associates, and they must report discovered breaches to the covered entity.

- Notification must generally be provided to the individual "without unreasonable delay" and in no event later than sixty (60) days after discovery

- Notification must always be provided to the Department of Health and Human Services if the breach involves more than 500 individuals; if less than 500 individuals, a report must be filed on an annual basis

- In addition to notification to HHS, if more than 500 individuals are involved in the breach, notification must be provided to prominent media outlets serving the respective area where the individuals reside

- ARRA increases the monetary penalties that could be applied to parties who violate the notification provisions

3. Missouri Data Breach Notification Statute Goes Into Effect

On July 9, 2009, Missouri joined 44 other states (including all contiguous states except Kentucky) in enacting what is commonly known as a "data breach notification statute." Although the statutes vary from state to state, their basic aim is to let people know if their personal information has been compromised, so they can take action to prevent identity theft. The classic example involves the theft of a laptop containing the names, addresses and social security numbers of all of a company's employees. Data breach notification statutes require the company to notify its employees that such security breach had occurred. Depending on the amount of personal information compromised, this can be a huge expense – not to mention a public relations nightmare.

The Missouri statute applies to "any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri." The Missouri law's definition of "personal information" is broader than many statutes because, in addition to including unique identification numbers created or collected by a government body (social security numbers, driver's license numbers, etc.) and financial access information (bank account numbers, credit card numbers, etc.), it also includes medical information and health insurance information.

In the event the security of such personal information is breached, the Missouri resident affected must be provided a notification "without unreasonable delay" that includes (i) a description of the incident in general terms, (ii) a description of the type of information obtained, (iii) a phone number the affected resident may call for further information or assistance (if one exists), (iv) contact information for consumer reporting agencies, and (v) advice to the resident to remain vigilant by reviewing account statements and monitoring free credit reports. The statute goes on to specify the means of notification and exceptions to the general rules (there are always exceptions). Failure to comply with the statute may expose you to an action by the Attorney General of Missouri seeking actual damages and a civil penalty not to exceed $150,000 per breach of security.

Obviously, the best practice, regardless of the Missouri legislation, is to implement effective protocols and procedures for handling personal information to reduce the risk of a security breach. If a resident's information is encrypted, redacted (no more than five digits of a social security number or four digits of a financial account) or otherwise altered by any method or technology in such a manner that the name or data

elements are unreadable or unusable, then a breach of security does not require notification because such altered information is not considered "personal information" under the statute.

If your company experiences an event which may be considered a data breach, we encourage you to contact either Jeb Bayer at *jbayer@polsinelli.com* or Tom O'Donnell at *todonnell@polsinelli.com*, as compliance with the Missouri statute, not to mention other state's statutes and federal statutes which may apply, is complicated. For example, the new personal health records and HIPAA rules discussed above may, in certain cases, pre-empt or alter the requirements under the Missouri statute.

Corporate Law Attorneys

Edward E. Frizell
816.360.4158
tfrizell@polsienlli.com

Jacob W. Bayer
816.374.0555
jbayer@polsinell.com

Alan C. Witte
314.889.7085
awitte@polsinelli.com

Zachary A. Abeles
314.889.7035
zabeles@polsinelli.com

Christopher S. Abrams
816.395.0602
cabrams@polsinelli.com

Orren S. Adams
314.889.7071
oadams@polsinelli.com

Vedrana Balta
816.360.4245
vbalta@polsinelli.com

John S. Black
816.374.0580
jblack@polsinelli.com

D. Al Boulware
816.374.0561
aboulware@polsinelli.com

Suzanne Bocell Bradley
816.364.2117
sbradley@polsinelli.com

Gerald W. Brenneman
816.360.4221
gbrenneman@polsinelli.com

Jared O. Brooner
816.364.2117
jbrooner@polsinelli.com

Paul J. Cambridge
314.552.6893
pcambridge@polsinelli.com

Jack M. Epps
913.234.7455
jepps@polsinelli.com

Geoffrey D. Fasel
816.360.4223
gfasel@polsinelli.com

Jennifer A. Feldhaus
314.889.7096
jfeldhaus@polsinelli.com

Brandon B. Fergerson
816.374.0540
bfergerson@polsinelli.com

Jeffrey E. Fine
314.552.6824
jfine@polsinelli.com

Robert E. Fitzgerald, Jr.
816.374.0534
rfitzgerald@polsinelli.com

Robert S. Goldstein
720.931.1164
rgoldstein@polsinelli.com

Larry K. Harris
314.889.7063
lharris@polsinelli.com

Judith S. Heeter
816.395.0640
judyheeter@polsinelli.com

Scott M. Herpich
816.360.4150
sherpich@polsinelli.com

Amy Hornbeck Abrams
816.572.4654
aabrams@polsinelli.com

Kyler L. Humphrey
314.889.7083
khumphrey@polsinelli.com

A. Drue Jennings
816.395.0603
djennings@polsinelli.com

Quentin L. Jennings
816.360.4108
qjennings@polsinelli.com

Paul G. Klug
314.552.6832
pklug@polsinelli.com

Philip N. Krause
816.691.3727
pkrause@polsinelli.com

Cortney E. Lang
816.572.4645
clang@polsinelli.com

John S. Larigan
816.360.4234
jlarigan@polsinelli.com

Glenn H. Lenzen
720.931.1179
glenzen@polsinelli.com

Scott A. Long
816.360.4229
slong@polsinelli.com

Gregory C. Lucas
816.364.2117
glucas@polsinelli.com

William W. Mahood III
816.360.4350
wmahood@polsinelli.com

Greg J. Mermis
816.395.0655
gmermis@polsinelli.com

Peter T. Moore
720.931.8152
pmoore@polsinelli.com

Anthony J. Nasharr
312.873.3611
anasharr@polsinelli.com

Michael C. O'Shaughnessy
816.360.4358
moshaughnessy@polsinelli.com

Bradley P. Pemberton
816.360.4224
bpemberton@polsinelli.com

Jay E. Pietig
816.360.4183
jpietig@polsinelli.com

James A. Polsinelli
816.360.4225
jpolsinelli@polsinelli.com

William E. Quick
816.360.4335
wquick@polsinelli.com

Mark J. Ross
816.360.4337
mross@polsinelli.com

Frank J. Ross Jr.
816.360.4167
fross@polsinelli.com

Michael A. Sabian
720.931.8153
msabian@polsinelli.com

Brian R. Salmo
314.622.6637
bsalmo@polsinelli.com

Nancy E. Saugstad
913.234.7425
nsaugstad@polsinelli.com

Lisa M. Schultes
816.360.4114
lschultes@polsinelli.com

Randal L. Schultz
816.374.0521
rschultz@polsinelli.com

Corporate Law Attorneys *(continued)*

Jeffrey H. Smith
816.572.4448
jsmith@polsinelli.com

Matthew J. Smith
314.552.6879
msmith@polsinelli.com

Chad C. Stout
816.572.4479
cstout@polsinelli.com

Kenneth H. Suelthaus
314.889.7001
ksuelthaus@polsinelli.com

Robert B. Sullivan
816.360.4151
rsullivan@polsinelli.com

Kelly Sullivan-Deady
816.360.4278
ksullivan@polsinelli.com

Carey Gehl Supple
816.395.0692
cgehlsupple@polsinelli.com

Lawrence A. Swain
913.234.7526
lswain@polsinelli.com

Chadd M. Tierney
816.360.4148
ctierney@polsinelli.com

Brian G. Wallace
816.360.4325
bwallace@polsinelli.com

Mark B. Weinheimer
618.692.2602
mweinheimer@polsinelli.com

Andrew M. Wilcox
816.360.4288
awilcox@polsinelli.com

Brian A. Wolf
913.234.7440
bwolf@polsinelli.com

Stanley N. Woodworth
913.234.7407
swoodworth@polsinelli.com

Kevin M. Zeller
816.572.4533
kzeller@polsinelli.com

Stuart H. Zimbalist
314.889.7052
szimbalist@polsinelli.com

About Polsinelli Shughart's Corporate Law Group

The Corporate Law attorneys at Polsinelli Shughart PC represent more than 5,000 business entities throughout the United States and abroad. We understand first hand both the challenges and rewards of growing from a startup to a mature business. We have helped shape many of our clients' paths to success over the years. As one of the fastest-growing law firms in the nation, we have matured and prospered with our clients. We make a concerted effort to try to understand our clients' businesses and the unique challenges of their particularly industry.

Our corporate attorneys often fill the role of "outside general counsel" to our clients, offering experienced counsel on the wide variety of legal issues you confront everyday. Our attorneys work hard to assemble the team of specialists who can address all of a client's legal needs as efficiently and cost-effectively as possible.

We build relationships with our clients, helping them develop and implement a variety of strategies critical to their ultimate success.

To learn more about our services, visit us online at www.polsinelli.com.

If you know of anyone who you believe would like to receive our e-mail updates, or if you would like to be removed from our e-distribution list, please contact Sarah Blair via e-mail at sblair@polsinelli.com.

About Polsinelli Shughart PC

With more than 470 attorneys, Polsinelli Shughart PC is a national law firm that is a recognized leader in the areas of business litigation, financial services, bankruptcy, real estate, business law, labor and employment, construction, life sciences and health care. Serving corporate, institutional and individual clients regionally, nationally and worldwide, Polsinelli Shughart is known for successfully applying forward-thinking strategies for both straightforward and complex legal matters. The firm can be found online at www.polsinelli.com.