



Personal Financial Information: Protection and Disclosure

by Tyler Novak and Jason Bushby

UPCOMING SEMINARS

October 15, 2008

2:00 p.m. – 3:30 p.m. ET

AllRegs Audioconference, Christian W. Hancock and D. Brian O'Dell will be speaking on "The Housing and Economic Recovery Act of 2008:

The Details You Need to Know"

To register, [click here](#).

October 22, 2008

The Alabama Bar Institute for Continuing Legal Education at the Cahaba Grand Conference Center - Birmingham, AL. H. Harold Stephens, President Elect, Alabama Defense Lawyers Association, will be speaking on Professionalism.

November 22, 2008

Alabama Defense Lawyers Association, Atlanta, GA. J.S. "Chris" Christie, Jr. will be speaking on "Preparing for and Prevailing at an Arbitration Hearing."

January 16, 2009

ABA TIPS Winter Meeting, Bonita Springs, FL. Paul P. Bolus will be speaking on the Status of Long Term Care litigation from a defendant's perspective.

Companies which regularly obtain, use and store consumer personal financial information are subject to federal and state regulations which prescribe the manner and ability of disclosing or sharing this sensitive information. Given the increased incidences of identity theft, making sure companies properly protect a consumer's personal financial information and prevent inadvertent disclosures are major concerns for consumers and regulators. This article is a practical guide designed to answer a few commonly asked questions we have received from companies about the disclosure and protection of consumer personal financial information.

What should my company do if there is an unauthorized disclosure of a consumer's personal information?

You should contact the company's counsel and work with counsel to determine the next appropriate step. Although, most states have adopted legislation mandating companies to notify its consumers about security breaches to consumer personal information, counsel should be engaged to assist in determining whether those laws apply to your company, whether they apply to the circumstances surrounding your breach, what should be contained in the notice, to whom the notice should be sent, and when the notice should be sent. Alabama has not yet adopted such legislation, but companies in Alabama should nonetheless contact their counsel to consider whether it is prudent to notify consumers of the breach. Additionally, under Alabama's Consumer Identity Protection Act, identity theft is a felony, so companies should also consider notifying law enforcement authorities immediately upon the discovery of a security breach involving consumer personal information. Alabama Code § 13A-8-190 et seq.

What steps must my company take to protect against identity theft?

By November 1, 2008, a company which meets the definition of a "financial institution" or "creditor" contained in the Fair Credit Reporting Act (FCRA), amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA), must develop and implement a written Identity Theft Program that is designed to detect, prevent and mitigate identity theft. Insurance companies do not fall under the definition of "financial institution" or "creditor." For more information on this FACTA legislation, see CFR § 681 et seq.

Can my company be civilly liable for an unauthorized disclosure?

Yes. Companies which are regulated by FACTA may be liable for negligent noncompliance in the amount of actual damages and willful noncompliance in the amount of actual, statutory and punitive damages. 15 U.S.C. § 1681c(g)..

Additionally, depending on whether a court rules that FACTA preempts a common law negligence claim, both companies which are not regulated by FACTA, as well as those which are, could be liable to a victim of identity theft for negligence. Whether such liability will attach depends on each state's tort law and the circumstances surrounding the breach. For example, some states, such as Alabama, recognize that when a special relationship is created or a special circumstance exists, a company could be subject to a lawsuit for negligent enablement of imposter fraud, resulting in the company having to pay substantial damages to the identity theft victim if the company failed to follow "commercially reasonable procedures".

What can my company do to limit its liability for an unauthorized disclosure?

Since a company's liability for an unauthorized disclosure, as stated above, could depend on whether the company took commercially reasonable procedures to protect against

continued on page 2

disclosure, there are steps a company should consider taking in an attempt to protect itself from liability. For example, companies should take full advantage of recent technology and purchase antifraud software which can help prevent identity theft of all variations. Also, companies should develop a procedure for shredding documentation which contains personal consumer information. Companies should also protect or limit access to such sensitive information by employees. Additionally, companies should ensure that all employees are trained on the proper procedures for using, storing and destroying such information. While taking these steps may not immunize your company from liability in a civil suit by a consumer for negligence, it could help to mitigate your damages.

When may a company disclose a consumer's personal financial information?

This threshold question derives primarily from the Gramm-Leach Bliley Act (GLBA) enacted by Congress in 1999. GLBA generally prohibits financial institutions (very broadly defined in the Act to include entities other than banks, such as insurance companies) from disclosing certain consumer information to an unaffiliated third party unless the financial institution follows GLBA's notice and opt out requirements. GLBA allows disclosure of information in the following instances:

- 1) where the disclosure is necessary to effect, administer or enforce a transaction (e.g., a financial institution provides financial information about a defaulting borrower to a third party for purposes of learning the location of the defaulting borrower);
- 2) with the consumer's consent;
- 3) to protect the confidentiality or security of your records pertaining to the consumer, service, product or transaction;
- 4) to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability (e.g., a financial institution provides information regarding a consumer's account balance to a business for purposes of determining whether the consumer has sufficient funds to cover a transaction with that third party business);
- 5) to certain agencies and persons assessing your compliance with industry standards, including your attorney, accountants and auditors;
- 6) to a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*);
- 7) to individuals or businesses with a legal interest relating to the consumer;
- 8) in connection with a proposed or actual sale, merger or acquisition; and
- 9) to comply with laws and legal process (e.g., a financial institution produces documents containing personal financial information about its consumers in response to a subpoena, court order or request for production (in the case where the institution is a plaintiff in civil litigation)).
- 10) Thus, financial institutions governed by GLBA may disclose information under one of the above-listed instances without complying with GLBA's notice and opt out requirements. In addition to GLBA, financial institutions should also keep in mind that states may also have legislation or regulations regarding the disclosure of consumer financial information. For example, Alabama has a banking regulation which specifically authorizes banks to disclose consumer information in response to a subpoena. Alabama Code § 5-5A-43.

This newsletter is sent to our friends as a courtesy of Bradley Arant. If you would prefer not to receive future e-mailings of this type, please email amccormick@bradleyarant.com.

Kay K. Bains
(205) 521-8220
kbains@bradleyarant.com

Stewart M. Cox
(205) 521-8276
scox@bradleyarant.com

Robert R. Maddox
(205) 521-8454
rmaddox@bradleyarant.com

Paul S. Ware
(205) 521-8624
pware@bradleyarant.com

Hope T. Cannon
(205) 521-8722
hcannon@bradleyarant.com

David W. Clark
(601) 592-9913
dclark@bradleyarant.com

J. Paul Compton, Jr.
(205) 521-8381
pcompton@bradleyarant.com

Jeffrey D. Dyess
(205) 521-8288
jdyess@bradleyarant.com

Ray D. Gibbons
(205) 521-8763
rgibbons@bradleyarant.com

N. Christian Glenos
(205) 521-8721
cglenos@bradleyarant.com

John E. Goodman
(205) 521-8476
jgoodman@bradleyarant.com

Joseph B. Mays, Jr.
(205) 521-8433
jmays@bradleyarant.com

J. Douglas Minor, Jr.
(601) 592-9973
dminor@bradleyarant.com

Andrew J. Noble, III
(205) 521-8342
anoble@bradleyarant.com

George R. Parker
(334) 956-7607
gparker@bradleyarant.com

David K. Pharr
(601) 592-9924
dpharr@bradleyarant.com

Dawn Helms Sharff
(205) 521-8200
dsharff@bradleyarant.com

James C. Smith
(704) 338-6010
jsmith@bradleyarant.com

H. Harold Stephens
(256) 517-5130
hstephens@bradleyarant.com

Charles A. Stewart, III
(334) 956-7608
cstewart@bradleyarant.com

Stephen L. Thomas
(601) 592-9912
stthomas@bradleyarant.com

Laurence D. Vinson, Jr.
(205) 521-8607
lvinson@bradleyarant.com

This newsletter is a periodic publication of Bradley Arant and should not be construed as legal advice or legal opinions on any specific facts or circumstances. The contents are intended for general information only, and you are urged to consult your own lawyer or other tax advisor concerning your own situation and any specific legal questions you may have. For further information about these contents, please contact your lawyer or any of the lawyers in our practice group.

Disclaimer and Copyright Information. 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."

©2008 Bradley Arant Rose & White LLP