

HEALTH LAW

Update

NEWS FOR THE CLIENTS AND FRIENDS OF BASS, BERRY & SIMS PLC

Red Flag for Healthcare Providers: The FTC's New Red Flag and Address Discrepancy Rules

October 8, 2008

Late last year, the Federal Trade Commission ("FTC") and other federal agencies issued final joint regulations entitled "*Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003*".¹ Little noticed by the healthcare industry when first issued, these regulations are now attracting significant attention because of their potential application to healthcare providers. The regulations implement parts of the *Fair and Accurate Credit Transactions Act of 2003* (the "Act") by imposing duties on certain entities regarding (i) the detection, prevention, and mitigation of identity theft (the "Red Flag Rules"), and (ii) responding to discrepancies in addresses for consumers on consumer reports (the "Address Discrepancy Rules"). While these regulations became effective January 1, 2008, compliance is mandatory by November 1, 2008.

Duties Regarding Identity Theft – Establishment of an Identity Theft Prevention Program

Healthcare providers are subject to the requirements of the Red Flag Rules regarding identity theft detection, prevention and mitigation if they meet a two part test. First, the healthcare provider must be a "creditor" as defined by the Red Flag Rules. A healthcare provider is a "creditor" for purposes of the Red Flag Rules if it regularly extends, renews or continues credit.² To illustrate, if a healthcare provider provides services for a patient but does not collect payment for such services when rendered, but instead defers payment such as by billing the patient, the healthcare provider is a creditor for purposes of the Red Flag Rules.³

¹ Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003. 72 Fed. Reg. 63717 et seq. (Nov. 9, 2007).

² For purposes of the Rules, the term "creditor" has the same meaning as in section 702 of the Equal Credit Opportunity Act, which defines the term as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C. § 1681a(r)(5).

³ An FTC representative, speaking informally at a recent AHLA teleconference, gave this example of the Red Flag Rules' application to healthcare providers. While typically government speakers do not purport to represent the official views of their agencies, their comments nonetheless can indicate how the agency might enforce the rule.

If a healthcare provider is a "creditor," then under the second prong of the Red Flag Rules test, the provider must determine if it offers or maintains "covered accounts" for its customers. To start with, an "account" is defined as a "continuing relationship established by a person with a...creditor to obtain a product or service for personal, family, household or business purposes," and includes "an extension of credit, such as...services involving a deferred payment..."⁴ An "account" is a "covered account" if it is (i) primarily for personal, family, or household purposes, and involves or is designed to permit multiple payments or transactions, or (ii) there is a reasonably foreseeable risk to customers or the safety and soundness of the...creditor from identity theft.⁵ These definitions are broad and could conceivably encompass the billing practices of many healthcare providers.

Healthcare providers that are both "creditors" and that offer or maintain "covered accounts" are required by the Red Flag Rules "to develop and implement a written [p]rogram that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account,"⁶ known as an Identity Theft Prevention Program ("Program").⁷ Each creditor must periodically reassess and determine whether it offers or maintains covered accounts, and if so, it must ensure that a Program is in place.⁸ The Red Flag Rules require the Programs to be centered on identity theft "Red Flags", which are patterns, practices, or specific activities that indicate the possible existence of identity theft.⁹ The required elements of each Program include reasonable policies and procedures to:

- (i) *Identify relevant Red Flags for the covered accounts that the...creditor offers or maintains, and incorporate those Red Flags into its Program;*
- (ii) *Detect Red Flags that have been incorporated into the Program of the...creditor;*
- (iii) *Respond appropriately to any Red Flags that are detected...to prevent and mitigate identity theft; and*
- (iv) *Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to its customers and to the safety and soundness of the...creditor from identity theft.*¹⁰

Each creditor must obtain approval of the initial Program by its board of directors, or if it does not have a board of directors, by a designated senior-level management employee.¹¹ The board or such employee must also be involved in the Program's development, implementation, administration, and oversight.¹² Staff must be trained as necessary to implement the Program,

⁴ 16 C.F.R. § 681.2(b)(1) (2008).

⁵ 72 Fed. Reg. at 63719.

⁶ 72 Fed. Reg. at 63724.

⁷ 16 C.F.R. § 681.2(d)(1) (2008).

⁸ 16 C.F.R. § 681.2(c) (2008). Creditors should take into consideration in making such a determination "(1) The methods it provides to open accounts, (2) The methods it provides to access its accounts, and (3) Its previous experiences with identity theft." *Id.*

⁹ 16 C.F.R. § 681.2(b)(9) (2008).

¹⁰ 16 C.F.R. § 681.2(d)(2) (2008).

¹¹ 16 C.F.R. § 681.2(e)(1) (2008).

¹² 16 C.F.R. § 681.2(e)(2) (2008).

and arrangements with third party service providers must be appropriately overseen to ensure compliance by such third party service providers with the Red Flag Rules.¹³

Each creditor required to implement a Program must use the Interagency Guidelines on Identity Theft, Prevention, and Mitigation (the "Guidelines") in developing its Program.¹⁴ These Guidelines are set out in an appendix to the Red Flag Rules, and a supplement to this appendix lays out categories and examples of Red Flags that creditors subject to the Red Flag Rules must consider including in their Programs as appropriate.¹⁵ Categories of Red Flags include the following:

- 1) *alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;*
- 2) *the presentation of suspicious documents;*
- 3) *the presentation of suspicious personal identifying information, such as a suspicious address change;*
- 4) *the unusual use of, or other suspicious activity related to, a covered account; and*
- 5) *notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the...creditor.*¹⁶

The Guidelines build upon the required elements of the Program outlined above and are intended to assist creditors in forming and maintaining a Program that meets the requirements of the Red Flag Rules.¹⁷

The Red Flag Rules allow for discretion and flexibility in the construction of the Program, and indicate that a Program should be appropriate to the size, complexity, nature and scope of the entity.¹⁸ Thus, a Program for a large hospital could be substantially different from that of a small physician practice. A healthcare provider covered by the Red Flag Rules could incorporate appropriate existing safeguards against identity theft, such as those already implemented for purposes of HIPAA compliance, as part of its Program and thus avoid duplicative processes.¹⁹

Duties Regarding Discrepancies in Addresses for Consumers

The Address Discrepancy Rules also impose certain requirements on users of consumer reports. Healthcare providers may use consumer reports, for example, to make decisions about credit for

¹³ 16 C.F.R. § 681.2(e)(3-4) (2008). A third party service provider, such as a billing service for a healthcare provider, may ensure that its activities "are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate identity theft" through its own program as long as it meets the requirements of the regulations, or a creditor could, by contract, require the services provider to have certain policies and procedures to detect, prevent, and mitigate identity theft. 72 Fed. Reg. 63732. For example, a healthcare provider subject to the Red Flag Rules could add provisions to its HIPAA Business Associate Agreement with such a third party service provider, or otherwise contractually obligate the provider to comply with the Red Flag Rules.

¹⁴ 16 C.F.R. § 681.2(f) (2008).

¹⁵ 16 C.F.R. § 681 Appendix A, Part II(c) (2008).

¹⁶ 16 C.F.R. § 681 Appendix A, Part II(c) (2008).

¹⁷ 16 C.F.R. § 681 Appendix A (2008).

¹⁸ 72 Fed. Reg. at 63724.

¹⁹ 16 C.F.R. § 681 Appendix A, Part I (2008). See also 72 Fed. Reg. at 63724.

patients or as part of background checks on employees. Some healthcare providers may be subject to the Address Discrepancy Rules without being subject to the Red Flag Rules requirements outlined above. The Act requires consumer reporting agencies ("CRAs") to notify users of consumer reports, which as mentioned could include hospitals or other healthcare providers ("Users"), of substantial discrepancies between the address provided by the User and the address on file with the CRA. The Address Discrepancy Rules provide guidance to Users regarding reasonable policies and procedures they should employ when they are notified of an address discrepancy.

Essentially, once a User receives a notice of address discrepancy, the User must have policies and procedures in place to enable the User to form a reasonable belief that the consumer report relates to the consumer about whom information was requested by the User from the CRA.²⁰ Such policies and procedures could include, for example, (i) comparing the information in the consumer report provided by the CRA with other information obtained by the User about the customer, and (ii) verifying the information in the consumer report with the consumer.²¹ The User must also have certain policies and procedures in place to enable it to provide what it reasonably determines to be the correct address of the consumer back to the CRA that initially provided the notice of address discrepancy.²²

Conclusion

The FTC has indicated that at this stage, its focus is less on penalizing creditors for failure to comply with these regulations and more on encouraging providers to make good faith efforts to comply.²³ Creditors should keep in mind that their Programs should be based on the risks of identity theft particular to their type of business. The risk of medical identity theft (theft of identity to obtain medical services) is a particular type of identity theft against which Programs of healthcare providers should guard.²⁴ The structure of these Programs is very flexible and in many cases could incorporate already existing policies and procedures, so long the Program is in accordance with the Guidelines. Please contact one of our attorneys in the Healthcare Practice Area listed below if you have any questions or would like additional information regarding these new rules.

²⁰ 16 C.F.R. § 681.2(c) (2008).

²¹ 16 C.F.R. § 681.2(c) (2008).

²² 16 C.F.R. § 681.2(d) (2008).

²³ The same FTC representative who informally gave the example of the Red Flag Rules' application to healthcare providers made this statement during the recent AHLA teleconference. *See* Footnote 3 *supra*.

²⁴ 72 Fed. Reg. at 63727.

Bass, Berry & Sims Healthcare Attorneys

H. Stanford Adams, Jr.
(615) 742-7775
sadams@bassberry.com

Philip F. Berg
(615) 742-7908
pberg@bassberry.com

Valere B. Fulwider
(615) 742-7742
vfulwider@bassberry.com

Anna Grizzle
(615) 742-7732
agrizzle@bassberry.com

Clevonne M. Jacobs
(615) 742-7769
vjacobs@bassberry.com

David King
(615) 742-7890
dking@bassberry.com

T. Scott Noonan, Co-Chair
(615) 742-6273
noonan@bassberry.com

Cynthia Y. Reisz
(615) 742-6283
creisz@bassberry.com

Catherine J.B. Sloan
(615) 742-7789
csloan@bassberry.com

Elizabeth S. Warren
(615) 742-7719
ewarren@bassberry.com

Kevin L. Alonso
(615) 742-7913
kalonso@bassberry.com

Krista Thornton Cooper
(615) 742-7734
kcooper@bassberry.com

Nesrin E. Garan
(615) 742-7903
ngaran@bassberry.com

Elisa E. Harris
(615) 742-6553
eharris@bassberry.com

J. James Jenkins, Jr.
(615) 742-6236
jjenkins@bassberry.com

Leslie Maclellan
(615) 742-7818
lmaclellan@bassberry.com

Brenda N. Phillips
(615) 742-6237
bnphillips@bassberry.com

Brian D. Roark
(615) 742-7753
broark@bassberry.com

Danielle M. Sloane
(615) 742-7763
dsloane@bassberry.com

Douglas M. Wolford
(615) 742-7917
dwolford@bassberry.com

H. Lee Barfield, II
(615) 742-6202
lbarfield@bassberry.com

Mary Beth Fortugno
(615) 742-7739
mfortugno@bassberry.com

Pooneh Ghiassi
(615) 742-7782
pghiassi@bassberry.com

Angela Humphreys
(615) 742-7852
ahumphreys@bassberry.com

Seth A. Killingbeck
(615) 742-7707
skillingbeck@bassberry.com

Claire F. Miley
(615) 742-7847
cmiley@bassberry.com

Shannon Pinkston
(615) 742-7727
spinkston@bassberry.com

Scott B. Shanker
(901) 543-5932
sshanker@bassberry.com

Leigh Walton, Co-Chair
(615) 742-6201
lwalton@bassberry.com

The materials contained herein have been abridged from the statutory sources and should not be construed or relied upon for legal advice. Readers are urged to consult legal counsel concerning particular situations and specific legal questions.

To ensure compliance with requirements imposed by the IRS, we inform you that this message is not intended to be used, and cannot be used, by the addressee or any other person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.

315 Deaderick Street • Suite 2700 • Nashville, TN 37238-3001 • (615) 742-6200
The Tower at Peabody Place • 100 Peabody Place, Suite 900 • Memphis, TN 38103-3672 • (901) 543-5900
1700 Riverview Tower • 900 S. Gay Street • Knoxville, TN 37902 • (865) 521-6200