

R. Timothy Columbus
202.429.6222
tcolumbus@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
Tel 202.429.3000
Fax 202.429.3902
steptoe.com

MEMORANDUM

June 18, 2009

TO: SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

**FROM: R.TIMOTHY COLUMBUS
JOHN FIELDING**

RE: APPLICABILITY OF RED FLAGS RULE TO SIGMA MEMBERS

I. QUESTIONS PRESENTED

- A. Whether the business activities of a member of the Society of Independent Gasoline Marketers of America (“SIGMA”) cause the member to be covered by the Federal Trade Commission’s (“FTC”) so-called Red Flags Rule.
- B. If a SIGMA member meets this threshold inquiry, what steps must be taken to comply with the Red Flag Rules regarding the detection, prevention, and mitigation of identity theft.
- C. What are a SIGMA member’s liabilities under the Red Flags Rule?

II. SHORT ANSWER

Whether a business is covered by the Red Flags Rule depends on whether its activities fall within the relevant definitions. SIGMA members are subject to the Red Flags Rule if they are “creditors” and if they own “covered accounts,” as those terms are used in the Rule. A SIGMA member is a creditor if it (1) offers its own fuel credit card or (2) extends credit by selling fuel to customers now and billing them later. A SIGMA member owns covered accounts if it (1) provides a fuel card account or (2) provides an account management system through

which customers remotely activate or deactivate fuel cards, change driver names, fueling permits, pin numbers, or add new units or order new cards. A SIGMA member who regularly extends credit to other businesses for goods or services is also subject to the requirements of the Rule, whether or not the other business later resells that good or service. Thus, a SIGMA member that is a creditor with one or more covered accounts must develop and implement a written program designed to detect, prevent, and mitigate identity theft. The program should be updated at least annually. What's more, if the member issues a fuel card, it must validate an address when it receives an address change notification for said account. Significantly, a SIGMA member may be subject to financial penalties for failing to comply with the Red Flags Rule.

The FTC has released a How-to Guide for businesses potentially affected by the Red Flags Rule. The FTC has also released a fill-in-the-blank form for businesses and organizations at low risk for identity theft. The online form offers step-by-step instructions for creating a written Identity Theft Prevention Program, and is available at <http://www.ftc.gov/redflagsrule>.

III. BACKGROUND

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act ("FACT Act"), amending the Fair Credit Reporting Act ("FCRA"). E.g., Peter L. McCorkell & Andrew M. Smith, Fair Credit Reporting Act Update-2008, 64 Bus. Law. 579 (2009). The FACT Act required the Federal Deposit Insurance Corporation ("FDIC"), the Board of Governors of the Federal Reserve System ("FRB"), the Office of the Comptroller of the Currency ("OCC"), the Office of Thrift Supervision ("OTS"), the National Credit Union Administration ("NCUA"), and the FTC (collectively, the "agencies") to jointly prescribe regulations requiring financial

institutions and credit grantors to adopt policies and procedures to identify patterns, practices, or specific activities that indicate the possible existence of identity theft (the “Red Flags Rule”). Id. The FACT Act also requires the agencies to adopt regulations requiring card issuers to adopt procedures to verify change of address requests followed in a short time by a request for a new or replacement card (the “Change of Address Rule”). Id. A separate provision of the FACT Act requires the agencies to issue jointly regulations requiring users of consumer reports to adopt policies and procedures for dealing with notices of address discrepancies received from consumer reporting agencies (the “Address Discrepancy Rule”). Id.

On November 9, 2007, the agencies published the final regulations under these provisions with a mandatory compliance date of November 1, 2008. The FTC has extended its deferral of enforcement of the Identity Theft Red Flags Rule to August 1, 2009. This delay is limited to the Identity Theft Red Flags Rule and does not extend to the Address Discrepancy Rule, or to the Change of Address Rule.

SIGMA is a national trade association representing independent chain retailers and marketers of motor fuel, both branded and unbranded. Specifically, a SIGMA member’s activities may include the management of (1) Automated Fueling Stations, whereby customers pay at the pump; (2) Mobile Refueling Operations, whereby a SIGMA member delivers fuel to its customers; and (3) Online Account Management Systems, whereby a SIGMA member provides a customer access to its accounts via the internet or telephone. SIGMA has expressed concern as to the FACT Act’s applicability to these activities. As such, SIGMA has asked us to determine whether these activities represent covered accounts, subject to regulation under the FACT Act and, if applicable, its duties and potential liabilities under the Act.

IV. DETERMINING WHETHER A SIGMA MEMBER HAS A DUTY UNDER THE RED FLAGS RULE

Title 16, Section 681 of the Code of Federal Regulations requires any “financial institution or creditor that offers or maintains one or more covered accounts [to] develop and implement a written Identity Theft Prevention Program (“Program”) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.” 16 C.F.R. § 681.1(d)(1). Whether a business or organization is covered by the Red Flags Rule is not based upon its industry or sector; instead, applicability is determined by “whether [its] activities fall within the relevant definitions.” Federal Trade Commission, Fighting Fraud with the Red Flags Rule: A How-to Guide for Business, (2009), available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf> [hereinafter How-to Guide].

A. Application of the Definition of a Creditor

The term “creditor” has the same meaning as in the Equal Credit Opportunity Act, 16 C.F.R. § 681.1(b)(5), which defines a creditor 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. § 1691a(e). The term “creditor” is broad; it includes “businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later.” How-to Guide, *supra*, at 9. Relevant examples of creditors include, but are not limited to, utility companies, health care providers, and

telecommunications companies. Id.; see also 16 C.F.R. § 681.1(b)(5) (referencing banks, finance companies, and automobile dealers).

A SIGMA member's operations do not necessarily make it a creditor. An automated fueling station pump may accept all major credit cards and national fuel cards. The FTC's How-to Guide states that

[s]imply accepting credit cards as a form of payment does not make you a "creditor" under the Red Flags Rule. But if a company offers its own credit card, arranges credit for its customers, or extends credit by selling customers goods or services now and billing them later, it is a 'creditor' under the law.

How-to Guide, supra, at 10. Additionally, a customer may prepay for goods or services or pay when goods or services have been rendered. The How-to Guide considers prepayment or payment when service is rendered as "non-credit accounts." Id. at 11. An example of a non-credit account is a pre-funded card, established by an initial wire transfer. All subsequent card transactions post directly against the deposited funds, working much like a debit card. Another example of a non-credit account is a deposit account, whereby customers submit a deposit to establish an initial credit line. The credit line is equal to the deposit provided, and clients are later billed (i.e., weekly or twice monthly) to the account. As such, in order for a SIGMA member to be considered a creditor, it would need to offer its own fuel credit card or extend credit by selling or delivering fuel to customers now and billing them later.

Moreover, whether a SIGMA member sells directly to a customer or to another business that then resells to a customer does not determine coverage under the Red Flags Rule. Whether a business is covered by the Red Flags Rule depends on whether its activities fall within the relevant definitions. Under the Rule, a "customer" means a person that has a covered account

with a creditor. 16 C.F.R. § 681.1(b)(6). Thus, a SIGMA member who regularly extends credit to other businesses for goods or services is subject to the requirements of the Rule, regardless if the other business later resells that good or service.

Being a “creditor” does not mean that a member would have to create a written program; however, as a creditor, the member would have to periodically conduct a risk assessment to help determine if it has acquired any covered accounts through changes to its business structure, organization, or processes.

B. Application of the Definition of Covered Accounts

Once a business or organization has concluded that it is a creditor, it must determine whether it has any “covered accounts.” There are two kinds of covered accounts. The first kind is any consumer-purpose account “designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, [or] utility account....” 16 C.F.R. § 681.1(b)(3)(i) (emphasis added). These consumer accounts are always “covered accounts.” How-to Guide, *supra*, at 11. As mentioned above, a company that issues its own credit card is deemed a creditor. For the purposes of this memorandum, a fuel card – allowing customers to purchase fuel now and pay later – should be deemed analogous to a credit card. Thus, any non-prepaid fuel card account should be treated as covered.

The second kind of “covered account” is any other account “for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or credit grantor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” 16 C.F.R. § 681.1(b)(3)(ii). Examples include “small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be

vulnerable to identity theft.” How-to Guide, supra, at 11. Unlike consumer accounts designed to permit multiple payments or transactions, other types of accounts are covered accounts “only if the risk of identity theft is reasonably foreseeable.” Id.

In determining whether an account is covered under the second category, the FTC recommends considering how an account is opened and accessed. Id. For example, “there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely – such as through the Internet or by telephone.” Id. A member’s operations do not necessarily implicate covered accounts because a customer may prepay for fuel delivery or pay when fuel delivery has been completed. Similarly, customers may use non-member fuel cards or credit cards at the member’s automated fueling stations. However, an online account management system accessible “24-hours a day from any computer that connects to the Internet,” presents a reasonably foreseeable risk of identity theft. Some fuel retailers provide online account management systems that allow customers to “activate or shut-off [fuel] cards and change driver names, fueling limits ... pin numbers” and “add new units or order new cards.” Id. If the member were to provide a similar online system, it would most likely possess covered accounts.

V. A SIGMA MEMBER’S DUTIES REGARDING THE DETECTION, PREVENTION, AND MITIGATION OF IDENTITY THEFT

If a SIGMA member’s accounts are considered to be covered accounts, the member must then comply with the Red Flags Rule. A credit grantor who offers or maintains one or more covered accounts must develop and implement a written Program designed to detect, prevent, and mitigate identity theft. 16 C.F.R. § 681.1(d)(1). Even when a business is considered low-

risk, if it has a covered account it must develop a written Program. How-to Guide, supra, at 12. Further, a low-risk business that has no covered accounts must periodically conduct a risk assessment to help “determine if [it has] acquired any covered accounts through changes to [its] business structure, processes, or organization.” Id.

The Program must be appropriate to the size and complexity of the entity and the nature and scope of its activities. 16 C.F.R. § 681.1(d)(1). The initial written Program must be approved by the board of directors or an appropriate committee of the board; involve the board of directors, an appropriate committee of the board, or a designated senior management employee in the oversight, development, implementation, and administration of the Program; provide for staff training to effectively implement the Program; and require effective oversight of service provider arrangements. 16 C.F.R. § 681.1(e)(1)-(4).

Importantly for SIGMA members, in designing its Program a creditor may incorporate its existing policies, procedures, and “other arrangements that control reasonably foreseeable risks to customers” and the creditor from identity theft. 16 C.F.R. pt. 681 app. A. This feature of the Red Flags Rule should allow the member to lower the overall costs of developing and implementing its Program.

A. The Program Must Identify Relevant Red Flags

A written Program must include reasonable policies and procedures to identify relevant situations that give rise to a reasonable suspicion of identity theft (“Red Flags”) and incorporate those Red Flags into its Program. 16 C.F.R. § 681.1(d)(2)(i). The member should consider the following factors in identifying relevant Red Flags: the types of covered accounts it offers or maintains; the methods it provides to open its covered accounts; the methods it provides to

access its covered accounts; and its previous experiences with identity theft. 16 C.F.R. pt. 681 app. A. The member's Program should also incorporate relevant Red Flags from the following sources: incidents of identity theft the member has experienced; methods of identity theft the member has identified that reflect changes in identity theft risks; and applicable supervisory guidance. Id. Finally, the member's Program should include relevant Red Flags from the following categories, as appropriate: alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; suspicious documents; presentation of suspicious personal identifying information, such as a suspicious address change; unusual use of, or other suspicious activity related to, a covered account; and 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 SIGMA member. Id.

In addition to the Red Flags Rule itself, the agencies have issued guidelines to assist covered entities in complying with the regulation, id., and have provided a list of "illustrative examples" of 26 Red Flags. See id. (Supplement). The agencies have stated that the list of Red Flags is not intended to be a "checklist" for bank examiners or covered entities. See Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718, 63745 (Nov. 9, 2007) (stating that listed red flags "are examples rather than a mandatory checklist"). The agencies also note that some of the listed Red Flags may not be relevant to a given situation while Red Flags in addition to those listed may be significant in other cases. Id.

B. The Program Must Detect Red Flags

A written Program must include reasonable policies and procedures to detect Red Flags that have been incorporated into the Program. 16 C.F.R. § 681.1(d)(2)(ii). For example, the member may obtain identifying information about, and verify the identity of, a person opening a covered account. 16 C.F.R. pt. 681 app. A. The member may also authenticate customers, monitor transactions, and verify the validity of change of address requests, in the case of existing covered accounts. Id. For online authentication, the FTC recommends considering the use of passwords, PIN numbers, smart cards, tokens, and biometric identification to authenticate customers. See How-to Guide, supra, at 23; see also “Authentication in an Internet Banking Environment” (Oct. 12, 2005), available at www.ffiec.gov/press/pr101205.htm.

C. The Program Must Prevent and Mitigate Identity Theft

A written Program must include reasonable policies and procedures to respond appropriately to any Red Flags that are detected and mitigate identity theft. 16 C.F.R. § 681.1(d)(2)(iii). Appropriate responses may include: monitoring a covered account for evidence of identity theft; contacting the customer; changing any passwords, security codes, or other security devices that permit access to a covered account; reopening a covered account with a new account number; not opening a new covered account; closing an existing covered account; not attempting to collect on a covered account or not selling a covered account to a debt collector; notifying law enforcement; or determining that no response is warranted under the particular circumstances. 16 C.F.R. pt. 681 app. A. In determining an appropriate response, the member should consider “aggravating factors” that may heighten the risk of identity theft, such as a “data security incident that results in unauthorized access to a customer’s account records”

held by the SIGMA member. Id. Such aggravating factors would “call for a stepped-up response because the risk of identity theft would go up.” How-to Guide, supra, at 24.

D. The Program Must Be Updated Periodically

A written Program must include reasonable policies and procedures to “[e]nsure that the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the ... creditor from identity theft.” 16 C.F.R. § 681.1(d)(2)(iv) (emphasis added). The Program should be updated based upon changes in methods of identity theft; the experiences of the financial institution or creditor with identity theft; changes in methods to detect, prevent, and mitigate identity theft; changes in the types of accounts that the financial institution or creditor offers or maintains; and changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements. 16 C.F.R. pt. 681 app. A. Section 681 does not define the term “periodically.” However, section 681 requires that the staff of the creditor report to the board of directors or appropriate senior employee regarding compliance “at least annually.” Id. This reporting requirement indicates that the member would need to update its Program at least annually.

E. The Member’s Duty Regarding a Change of Address

If a SIGMA member issues a fuel card, it has additional duties under the Change of Address Rule. Section 681 requires that a card issuer establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer’s debit or credit card account and, within 30 days after receiving notification, the card issuer receives a request for an additional or replacement card for

the same account. 16 C.F.R. § 681.2(c). A “card issuer” is defined as a person that issues a debit or credit card. 16 C.F.R. § 681.2(a). As mentioned above, this memorandum considers a fuel card analogous to a credit card. Should the member receive a notification of a change of address and a request for a new fuel card for the same account within 30 days of each other, it may not issue an additional replacement card until it notifies the cardholder of the request (at the cardholder’s former address or by any other means of communication that the member and the cardholder have previously agreed to use) and provides to the cardholder a reasonable means of promptly reporting incorrect address changes. 16 C.F.R. § 681.2(c). The member may otherwise assess the validity of the change of address in accordance with the policies and procedures it has established pursuant to section 681.1. Id. Alternatively, the member may satisfy the requirements of section 681.2(c) if it validates an address when it receives an address change notification before it receives a request for an additional replacement card. 16 C.F.R. § 681.2(d). Note that any electronic or written notice the member provides to a cardholder must be “clear and conspicuous” and must be provided separately from any regular correspondence with the cardholder. 16 C.F.R. § 681.2(e). Section 681.2 defines “clear and conspicuous” as “reasonably understandable and designed to call attention to the nature and significance of the information presented.” 16 C.F.R. § 681.2(b)(2). At a minimum, the member needs to validate an address when it receives an address change notification.

F. Liability Under the Red Flags Rule

The proper development and implementation of a written Program designed to detect, prevent, and mitigate identity theft will allow the member to avoid financial penalties. The FTC has stated, “Although there are no criminal penalties for failing to comply with the Rule,

violators may be subject to financial penalties.” E.g., Steven Toporoff, Franchisors: Are You Complying with the Red Flags Rule’s New Requirements for Fighting Identity Theft?, May 2009, <http://www.ftc.gov/bcp/edu/pubs/articles/art14.shtm>. Under the Red Flags Rule, creditors are subject to administrative enforcement of the FCRA by the FTC pursuant to Title 15, Section 1681s(a)(1) of the United States Code. 16 C.F.R. § 681.1(a). Section 1681s provides

“In the event of a knowing violation, which constitutes a pattern or practice of violations of this title ... the Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person.... In such action, such person shall be liable for a civil penalty of not more than \$2,500 per violation.”

15 U.S.C. 1681s(a)(2)(A). Section 1681s also states, “In determining the amount of a civil penalty under subparagraph (A), the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.”

VI. CONCLUSION

Whether a business is covered by the Red Flags Rule depends on whether its activities fall within the relevant definitions. SIGMA members are subject to the Red Flags Rule if they are “creditors” and if they own “covered accounts,” as those terms are used in the Rule. The member is a creditor if it (1) offers its own fuel credit card or (2) extends credit by selling fuel to customers now and billing them later. Likewise, the member owns covered accounts if it (1) provides a fuel card account or (2) provides an account management system through which customers remotely activate or deactivate fuel cards, change driver names, fueling permits, pin numbers, or add new units or order new cards. Should the member own covered accounts, it must develop and implement a written program (approved by its board of directors or an

appropriate committee of the board) designed to mitigate identity theft in connection with the opening of a covered account or any existing covered account. The member must also assess its program—at least annually—to ensure it remains current. What’s more, if the member issues a fuel card, it must validate an address when it receives an address change notification. Even so, the member may incorporate its existing policies and procedures into its program, lowering its overall implementation costs. Although there are no criminal penalties for failing to comply with the Red Flags Rule, the member may be subject to monetary penalties should it violate the Rule.

If you have additional questions regarding this matter, please contact Tim Columbus: 202-429-6222 or John Fielding: 202-429-6296 at Steptoe & Johnson.