BEFORE THE
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

	)	
	)	
The Red Flags Rule	)	Project No. R611019
	)	
	)	

COMMENTS OF VERIZON

Michael E. Glover
Of Counsel

Karen Zacharia
Joshua E. Swift
Verizon
1515 North Courthouse Road, Suite 500
Arlington, VA 22201
(703) 351-3039

John T. Scott, III
Verizon Wireless
1300 I Street, N.W., Suite 400-West
Washington, D.C. 20005
(202) 589-3760

Kirk J. Nahra
Amy E. Worlton
Wiley Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000

September 18, 2006

BEFORE THE
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

The Red Flags Rule	)	Project No. R611019

COMMENTS OF VERIZON

I. INTRODUCTION

As the Federal Trade Commission ("Commission" or "FTC") and the other Joint Agencies currently recognize, companies such as Verizon[1] that would be subject to the Red Flags Rule already have sophisticated policies and procedures in place to help prevent identity theft and other types of fraud.[2] Verizon generally supports the proposed Red Flags Rule. But while the proposed guidelines and regulations allow some amount of flexibility, the Joint Agencies should modify the proposed Rule as discussed below to provide maximum flexibility within the boundaries of the Fair Credit Reporting Act ("FCRA").[3] Flexibility is necessary in order for businesses to respond effectively to

[1] The Verizon companies participating in this filing ("Verizon") are the regulated wholly owned subsidiaries of Verizon Communications Inc. and Cellco Partnership, d/b/a/ "Verizon Wireless." Unless otherwise noted, in this filing, the term "Verizon" includes Verizon Wireless.

[2] Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, Federal Trade Commission (collectively, "Joint Agencies"), Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40786, 40791 (July 18, 2006) ("*Joint NPRM"*).

[3] 15 U.S.C. § 1681 *et seq.*

identity theft based on their unique risk profiles and existing policies and business processes.

II. THE FTC AND THE OTHER JOINT AGENCIES SHOULD ADOPT A FLEXIBLE RED FLAGS RULE THAT ALLOWS A COMPANY TO ADDRESS IDENTITY THEFT CONSISTENT WITH ITS UNIQUE RISKS AND EXISTING ANTI-FRAUD PROGRAMS.

A. The Joint Agencies need not define the term "account," but in no event should they define "account" to include closed accounts.

Verizon urges the Joint Agencies not to define the term "account." Adopting the proposed definition of "account" would create confusion and is not necessary in order to identify the activities subject to the Red Flags Rule. In any case, defining "account" to include "closed accounts" would significantly and unnecessarily disrupt existing business processes.

The proposed definition fails to provide the "ease of reference" sought by the Joint Agencies, and instead, creates confusion.[4] The *Joint NPRM* defines "account" as "a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k)."[5] Many creditors that are subject to FCRA are not in the business of providing financial products or services defined under section 4(k) of the Bank Holding Company Act. Accordingly, the proposed definition of "account" appears

[4] *Joint NPRM* at 40789.

[5] *Id.* at 40823-24 (proposed 16 C.F.R. § 681.2(b)(1)).

not to encompass some creditors, although the Joint Agencies plainly intend the Red Flags Rule to apply to such creditors.

Moreover, the Joint Agencies need not define "account" in order to clarify which entities and activities are subject to the Red Flags Rule. Indeed, as the Agencies recognize, the underlying statute, the Fair and Accurate Credit Transactions Act ("FACTA"), does not define the term "account."[6] Definitions of "financial institution" and "creditor" already referenced in FCRA are long-standing and well-understood statutory terms.[7] Additional "thresholds" to the application of the Rule would be redundant at best and would risk introducing conflicts with the settled statutory framework.

Nonetheless, if the Joint Agencies decide to adopt a definition of "account," the term should be limited to continuing customer relationships, not closed accounts. Otherwise, significant implementation difficulties could arise. Some of Verizon's business units have policies and procedures in place to close certain delinquent accounts and turn over their collection to outside collection agencies. Subsequently, with respect to these accounts, outside collection agencies, not Verizon, receive information from and relay information to credit reporting agencies. Outside collection agencies do not report credit report information back to Verizon with respect to such accounts. Accordingly, if the Red Flags Rule applied to closed accounts, Verizon would incur substantial developmental costs to overhaul its reporting arrangements with outside collection

[6] *See id.* at 40789; *see also* the Fair and Accurate Credit Transactions Act ("FACTA"), Pub. L. No. 108-159, § 114, 117 Stat 1952, 1959 (2003).

[7] *See* 15 U.S.C. §§ 1681a(r)(5) (defining "creditor" by reference to the definition of that term in the Equal Credit Opportunity Act, 15 U.S.C. § 1691a(e)); 1681a(t) (defining "financial institution").

agencies in order to ensure Verizon's compliance. There is no policy reason to require this outcome, as outside collection agencies likely themselves will be subject to the Red Flags Rule, and consumers would still be protected under FCRA.[8]

B. The definition of "customer" should not be used to improperly expand the jurisdiction of the FCRA.

The Joint Agencies propose to broaden the definition of "customer" to encompass any "person," as defined by FCRA as any "individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or any other entity."[9] FCRA, however, does not use the definition of "person" to identify the class of protected persons (which are "consumers"), but rather, to identify the class of regulated persons.[10] Neither FCRA nor the Red Flags Rule promulgated pursuant to that statute are intended to protect small business.[11] For that reason, the Red Flags Rule definition of "customer" should be equivalent to that in the FCRA – namely, an "individual."[12]

---

[8] *See, e.g.,* 15 U.S.C. § 1681j(a) (granting consumers the right to obtain their credit report free of charge on an annual basis so they may review it for signs of identity theft).

[9] *Joint NPRM* at 40790; *see* 15 U.S.C. § 1681a(b).

[10] *See, e.g.,* 15 U.S.C. 1681m(a) (requiring a "person" to provide the "consumer" with notice of any adverse action taken on the basis of a consumer report).

[11] *See, e.g.,* 15 U.S.C. §§ 1681(a)(4) (Congress found that "[t]here is a need to insure that *consumer* reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the *consumer's* right to privacy") (emphasis added); 1681a(c) ("The term 'consumer' means an individual.").

[12] *Id.*

C. Senior Management approval of Identity Theft Prevention Programs should be sufficient.

The FTC and the other Joint Agencies should adopt a flexible approach allowing for senior management approval of Identity Theft Prevention Programs. But the Agencies should not adopt the proposed rule requiring approval of the Program by the Board of Directors.[13] The Agencies note that the "Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities."[14] That flexibility must extend not only to small creditors, but also to large public companies. Because creditors are ultimately responsible for complying with the Red Flags Rule, creditors should be able to determine the appropriate level of approval and oversight of Programs.

Verizon's corporate structure includes a senior management supervisory function that would not require the direct involvement of the Board of Directors to approve an Identity Theft Prevention Program. Verizon has implemented an enterprise-wide Corporate Compliance Program, with participation from each Verizon business unit. The Corporate Compliance Program is overseen by the Chief Compliance Officer and a Corporate Compliance Council. The Chief Compliance Officer reports quarterly to the Verizon Management Audit Committee and annually to the Audit and Finance Committee of the Verizon Communications Board of Directors. Approval and monitoring of any Identity Theft Prevention Program could be appropriately handled by the Chief Compliance Officer and his compliance staff, in conjunction with the Corporate

[13] *See Joint NPRM* at 40789, 40793, 40824 (proposed 16 C.F.R. § 681.2(d)(5)).

[14] *Id.* at 40788.

Compliance Council, just like most other compliance matters. Senior management has the expertise and day-to-day contacts necessary to oversee a comprehensive Identity Theft Prevention Program and ensure that it adapts quickly to emerging fraud threats.

D. The Agencies should clarify obligations with respect to "precursors" of identity theft

The Joint Agencies state that the definition of "Red Flag" will "include those precursors to identity theft which indicate 'a possible risk' of identity theft to customers, financial institutions, and creditors."[15] However, it may be burdensome and unnecessary to require that companies respond to such precursors of identity theft in the same way that they respond to Red Flags that are more indicative of actual, on-going identity theft. For example, does a single complaint of an alleged "phishing" scheme trigger a requirement to revise the Identity Theft Prevention Program? Is a creditor required independently to seek out evidence of a "precursor"? Is a creditor required to subscribe to third party services to monitor the possibility of precursor activity?

The Joint Agencies should clarify that companies subject to the Red Flags Rule: (a) have no affirmative obligation to monitor for "precursors" of identity theft, but rather, have a duty to respond to reasonable evidence of identity theft that might arise; and (b) have discretion over their responses to "precursors," which should be based on a company's assessment of identity theft risks, but which may differ in scale and kind from a company's response to clear and specific signals of identity theft.

[15] *Id.* at 40790.

E. The Joint Agencies should clarify obligations concerning third-party computer-based products.

The FTC and the other Joint Agencies should clarify that the term "third party computer-based programs" refers specifically to identity theft detection *software* that could be used by Verizon in-house or by a third party vendor. In the *Joint NPRM*, the Joint Agencies state that companies subject to the Red Flags Rule must "independently assess" the compliance of such programs with the Rule and may not "rely solely on the representations of the third party."[16] Verizon seeks clarification that the term "third party computer-based programs" does not also refer to services provided by outside vendors specializing in fraud risk management, a topic treated differently elsewhere in the proposed Red Flags Rule.

Also, the *Joint NPRM* is not clear about the degree to which creditors must monitor "third party computer-based programs."[17] The Commission and the other Joint Agencies should clarify that, once a company forms a reasonable belief that a third-party program adheres to the company's Identity Theft Prevention Program: (a) the Red Flags Rule does not require the company to make a case-by-case "independent assessment" of a third-party program's findings concerning a particular account; and (b) the company may rely solely on such specific findings.

F. Examples of compliance measures and the sum of Appendix J Red Flags should not effectively become enforcement benchmarks.

The Joint Agencies should continue to acknowledge that creditors have discretion in determining which Red Flags are appropriate for their businesses. Further, the

[16] *Id.* at 40791.

[17] *See id*. at 40791-92.

Agencies should expressly state that the enumerated compliance examples and the body of Red Flags in the *Joint NPRM* are provided merely as an aid to companies subject to the Red Flags Rule. The Agencies should clarify that that the examples and Red Flags do not represent a compliance benchmark, as compliance must be based on a company's individual risk assessment and implementation of an Identity Theft Prevention Program within a company's existing anti-fraud policies and procedures.

The Joint Agencies request comment on whether proposed examples of how to prevent and mitigate identity theft should be included in the Red Flags Rule and whether additional measures should be included.[18] In addition, the Joint Agencies ask whether the Red Flags included in Appendix J are too specific, not specific enough, or incomplete.[19] Finally, the Joint Agencies request comment on whether to include examples of measures to reasonably confirm the accuracy of the consumer's address or whether different or additional examples should be listed.[20] The Joint Agencies note that these measures are "illustrative,"[21] that Appendix J is "not meant to be exhaustive,"[22] and that companies must adopt into their Identity Theft Prevention Programs only the "relevant Red Flags."[23]

As the Joint Agencies recognize, companies must have the flexibility to consider the risk factors of their businesses and the appropriate measures necessary to implement

---

[18] *Id.* at 40793.

[19] *Id.* at 40794.

[20] *Id.* at 40796.

[21] *Id*. at 40792, 40796.

[22] *Id.* at 40794.

[23] *Id.* at 40824 (proposed 16 C.F.R. § 681.2(d)(1)(ii)).

an effective Identity Theft Prevention Program given those risk factors. Accordingly, companies subject to the Red Flags Rule should not be compelled to implement an example measure or include a certain Red Flag in the company's Program based on the fear that failure to do so will be construed as a Red Flags Rule violation. If that were the case, companies would effectively be bound by the examples, which may not be appropriate to a particular company or industry and which may represent an inefficient application of compliance resources.

Verizon has concerns that many of the Red Flags are poorly-suited to its business and would disrupt existing processes without correspondingly reducing identity theft risks. Verizon should have a meaningful choice not to adopt these Red Flags and instead pursue alternative identity theft prevention measures. Verizon's chief concerns with respect to proposed Red Flags are as follows.

Implementing some of the Red Flags would unnecessarily burden consumers applying for Verizon services and cause undue delays in providing such services:

- *Red Flag 15.* Verizon tries to streamline service applications in order to minimize burdens on consumers, regardless of whether they sign up by telephone, online or in person. Thus, Verizon generally does not ask for information beyond what normally would be available from a wallet or consumer report. Requiring more information in response to Red Flag 15 would substantially burden both consumers and Verizon business units, without materially adding to the ability of existing credit checks to detect identity theft.
- *Red Flag 3.* When a consumer applies for service from Verizon, credit screening generally occurs automatically. But these automatic processes would not reveal

the patterns of suspicious activity contemplated by Red Flag 3. Thus, Verizon would need to implement costly manual reviews of new customers' entire credit reports, which would impose substantial delays. Such manual processes would provide little additional protection from identity theft, as Verizon already has implemented many fraud prevention measures within its business processes. For example, Verizon halts processing of new customers' service applications if automatic reviews of consumer reports reveal any one of a number of fraud alerts FCRA already requires consumer reports to include.[24]

In other cases, due to the nature of its business, Verizon simply is not situated to implement a Red Flag measure:

- *Red Flag 4*. In some Verizon business units, a customer initiating service will fax identifying documents. The quality of faxed copies is normally inadequate for detecting a suspicious alteration, and accordingly, for these business units, Red Flag 4 would not be an efficient use of compliance resources.
- *Red Flag 5.* Some Verizon business units do not have face-to-face contact with customers. Thus, these business units would not have an opportunity to comply with Red Flag 5 by comparing the photographic or physical description of a person appearing on identification documents with the person presenting those documents.
- *Red Flag 8, Subpart b.* In Verizon's experience, credit reporting agencies do not always report information in the Social Security Administration's Death Master

[24] *See, e.g.,* 15 U.S.C. § 1681c(h) (notices of address discrepancy); § 1681c-1(c) (active military duty alert).

File. Thus, integrating such information into Verizon's application and credit check processes would be prohibitively costly.

Other proposed Red Flags, if they effectively became requirements on Verizon, would necessitate treating certain everyday events as indicia of identity theft. In Verizon's case, the return of mail sent to customers (Red Flag 17) or a failure of a customer to make timely payment (Red Flag 18, subpart b and Red Flag 19, subpart a) are common occurrences and do not suggest identity theft. In the former case, Verizon generally attempts to find an updated address, and in the latter, to obtain payment. While Verizon could uncover evidence of identity theft in the course of these attempts, the simple fact of returned mail or non-payment should not generate any obligations for Verizon.

Finally, Verizon supports the proposal to move Appendix J to the end of the relevant part for ease of use.[25]

G. Creditors should have maximum flexibility in managing service provider relationships.

The Commission and the Joint Agencies need not address in the Red Flags Rule the details of the relationship between creditors and service providers. The Joint Agencies have already acknowledged that a service provider could comply either with a creditor's Identity Theft Prevention Program, or it could utilize its own Program to prevent identity theft.[26] However, if a creditor requires a service provider to comply with the creditor's Program, that fact should be taken into account when assessing whether a

[25] *See Joint NPRM* at 40794.

[26] *See id*. at 40793.

creditor is compliant. In other words, service providers should not be required to adopt a creditor's Program, but where a creditor bargains with a service provider to so tailor its activities to the creditor's unique risk profile, the Joint Agencies should recognize that identity theft risks are reduced accordingly.

H. The Joint Agencies should retain the proposed flexible position with regard to inactive accounts.

Verizon supports the Joint Agencies' flexible approach with respect to whether new activity in an account that has been inactive indicates possible identity theft. As the Joint Agencies rightly recognize, new activity may or may not be meaningful depending upon the type of account and expected patterns of usage.[27] The Joint Agencies inquire whether they should adopt this flexible approach by creating a Red Flag, or whether they should instead promulgate a binding regulation based on Section 114 of FACTA,[28] which directs the Joint Agencies to consider requiring customer notification if activity occurs in an account that has been inactive for at least two years.[29] In Verizon's case, because it generally provides and bills for service on a monthly basis, accounts that are open should be considered "active," and the notion of two years' inactivity would not normally apply. Thus, adopting a flexible Red Flag is the appropriate approach, as opposed to imposing a rigid two year clock that may not translate to all types of businesses.

---

[27] *Id.* at 40794.

[28] Pub.L. 108-159 § 114, 117 Stat 960.

[29] *Joint NPRM* at 40794.

I. The Joint Agencies should adjust requirements for timeliness.

Verizon urges the FTC and the other Joint Agencies to require responses to notices of address discrepancies "promptly," but not necessarily in the same "reporting period."[30] The Joint Agencies do not define "reporting period," creating uncertainty as to what the proposed rule would require. A "reporting period" would seem to indicate a "batch" transmission of data from a creditor to a credit reporting agency occurring at regular intervals. However, many Verizon entities do not "batch" disclosures to credit reporting agencies in regular reporting periods, but instead maintain real-time "live feeds" with these agencies. The term "reporting period" sits uneasily with "live feeds," as there may be only seconds between the establishment of an account or verification of customer identity and the next transmission to a credit reporting agency. The duty to respond "promptly" will allow companies to meet the spirit of the Red Flags Rule while acknowledging these business realities.

III. CONCLUSION

The Commission and the other Joint Agencies should modify the proposed Red Flags Rule as set forth in these comments so that companies subject to its guidelines and requirements will have broad discretion to determine how best to implement the Rule into their policies and procedures.

[30] *Id.* at 40823 (proposed 16 C.F.R. § 681.1(d)(3)).

Respectfully submitted,

/s/

_____

Michael E. Glover
Of Counsel

Karen Zacharia
Joshua E. Swift
Verizon
1515 North Courthouse Road, Suite 500
Arlington, VA 22201
(703) 351-3039

John T. Scott, III
Verizon Wireless
1300 I Street, N.W., Suite 400-West
Washington, D.C. 20005
(202) 589-3760

Kirk J. Nahra
Amy E. Worlton
Wiley Rein & Fielding LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000

September 18, 2006