SECURITIES AND EXCHANGE COMMISSION

Suggested Amendments to the
Securities and Exchange Commission's
Current Rules for Safeguarding Consumer Report Information
File No. S7-33-04, RIN 3235-AJ24

Comments Submitted By: Ms. Cheryl A. Tedder
Villanova University School of Law

Comments Submitted Electronically on November 23, 2004

Comments Submitted To: Mr. Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 Fifth Street, NW
Washington, DC 20549-0609

Date: November 23, 2004

I. Introduction

I welcome this opportunity to submit these comments in response to the Securities and Exchange Commission's ("Commission") request for public comments regarding the proposed implementation of Section 216 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), which requires financial service providers to implement written policies and procedures that provide for the proper disposal of consumer report information and records. I write on my own behalf as an investor and third-year law student at the Villanova University School of Law to express my concerns that my personal and financial information could still become available to unknown persons even though safeguard policies and procedures may be in place. While I am aware that the deadline for comment submissions has passed, I would nonetheless appreciate the Commission's consideration of the recommendations that follow.

The following comments discuss what I feel are potentially serious implications of the ambiguity in the Commission's proposed definitions, including the proposed "reasonableness" standard, to offer my support for the Commission's proposal that all safeguard and disposal

policies and procedures be in writing, and to suggest that the Commission delineate more specific standards for safeguarding customer information. In Section II, I briefly describe the proposed rule and the issues on which the Commission seeks public comments. Section III contains a more detailed discussion of my position on the proposed definitions, the necessity of putting policies and procedures in writing, and the potential pitfalls of leaving the existing safeguard rule as-is. Section IV contains a brief conclusion.

II. Background

Section 216 of the FACT Act requires the Commission to "adopt regulations [that require] any person who maintains or possesses a consumer report or information derived from a consumer report for a business purpose [to] properly dispose of the information."[1] One purpose of §216 is to prevent the unauthorized disclosure and use of private personal and financial information contained in a consumer report.[2] Furthermore, §216 is meant to reduce the risk of identity theft and other fraudulent crimes "by ensuring that records containing sensitive [consumer] information are appropriately redacted or destroyed before being discarded."[3]

The Commission is one of seven agencies obligated to promulgate regulations to carry out the goals of §216.[4] Those subject to the Commission's final disposal rule include brokers, dealers, investment companies, and those investment advisers currently registered with Commission

---

[1] *See* 69 Fed. Reg. 56,304 (proposed Sept. 20, 2004) (to be codified at 17 C.F.R. pt. 248) [hereinafter Fed. Reg.].

[2] *See id*. (citing 108 Cong. Rec. S13,889 (Nov. 4, 2003)).

[3] *See id*. (quoting Senator Nelson).

[4] *See id*. The other six agencies are the Federal Trade Commission ("FTC"), the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation ("FDIC"), the Office of Thrift Supervision, and the National Credit Union Association.

("covered entities" or "financial service providers").[5] In adherence to its duties under §216, the Commission's proposed rule requires financial service providers to take reasonable measures to adopt and implement in-house polices and procedures to properly dispose of the consumer report information within their possession.

Among the issues on which the Commission seeks public comments is the adequacy of the proposed definitions of terminology to be used in the final rule. Further, the Commission seeks comments on whether the disposal policies and procedures adopted by financial service providers as a result of this rule should be in writing. Finally, the Commission seeks comments on whether modifications should be made to the existing safeguard rule to allow for increased specificity, and require that a covered entity's safeguard policies and procedures also be in writing. As the following discussion demonstrates, I agree that the disposal and safeguard policies and procedures should be in writing, and modifications should be made to the existing safeguard rule. However, the Commission's proposed definitions remain lacking in specificity and should be clarified in the final rule.

III. Discussion

The proposed rule is an excellent attempt by the Commission to create much needed protections for non-public consumer report information. The rule is inadequate, however, because it contains too much ambiguity. As the discussion in Section A demonstrates, the proposed definitions are over-broad and must be clarified before being implemented to avoid unnecessary confusion and prevent unnecessary expenditures on compliance.

Furthermore, it is imperative that covered entities be required to put their disposal policies and procedures in writing. As discussed in Section B, written policies and procedures provide better guidance, they are more difficult to change, and they better enable the Commission to oversee that the policies and procedures are actually being carried out.

Finally, the Commission should modify its existing safeguard rule to require covered entities to include

[5] *See id*. at 56,305.

certain elements in their policies and procedures for protecting their customer information. As demonstrated in Section C, having increased specificity in their safeguard policies and procedures will better enable covered entities to know how to safeguard customer information, and will indicate when those entities might be liable if they fail to adhere.

A. The Commission's Proposed Definitions Are Too Ambiguous and the Language of the Rule Is Over-Broad

The language of a statute, or an agency's interpretation of that statute, is considered ambiguous by the courts when the language is susceptible to multiple interpretations.[6] Ambiguity in a proposed rule exists when the language of the rule creates confusion among those subject to the rule and obligated to carry out its requirements. In the present case, several of the Commission's proposed definitions are susceptible to multiple interpretations: (1) the definition of "disposal," (2) the definition of "reasonableness," and (3) the definition of "business purpose." Furthermore, the definition of "consumer report information" should be clarified to except publicly available information. Because a finding of ambiguity requires the court to determine whether and what kind of deference should be accorded an agency's interpretation of the statute it is trying to implement,[7] I urge the Commission to re-evaluate its proposed definitions before implementing the final rule.

1. Definition of "Reasonable Measures"

While the proposed "reasonable measures" standard provides much needed flexibility to covered entities

---

[6] *See* Specialty Ins., et al. v. Royal Indemnity Co., 2004 U.S. Dist. LEXIS 13376, at *10 (describing plaintiff's contention that language is ambiguous because "it is 'reasonably susceptible to different constructions and capable of being understood in more than one sense.'").

[7] *See* N.Y. State Bar Ass'n v. FTC, 276 F.Supp.2d 110, 136-37 (D.D.C. 2003) (citing Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837, 843 (1984)).

charged with implementing disposal policies and procedures, it is still over-broad and too ambiguous in its definition. In its current form, the standard requires: "any covered entity that maintains or otherwise possesses consumer report information [to] 'take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.'"[8] Financial service providers vary tremendously in size and resource-base, so an across-the-board uniform standard would be unrealistic and impossible for all providers to adhere to. The advantages of this flexibility, however, could be undermined by the confusion and uncertainty created by the ambiguity of the standard. While it is important that financial service providers consider "the sensitivity of the consumer report information, the size of the entity and the complexity of its operations, the costs and benefits of different disposal methods, and relevant technological changes" as the Commission suggests,[9] it remains unclear, even with the Commission's examples, when the methods of disposal of the information will be reasonable.

It is possible to establish a more stringent standard while still maintaining flexibility. First, the Commission must clarify how covered entities are to gauge the "sensitivity of the consumer report information." As one commentator points out, in passing the FACT Act, Congress clearly decided that all information contained in or derived from consumer reports "is sufficiently sensitive to require proper disposal."[10] The language of the "reasonable measures" standard, however, fails to account for those entities that might decide whatever consumer report information they have is not sufficiently sensitive to require proper disposal under this rule. Thus, in its final rule the Commission must specify that all covered entities are required to properly dispose of all consumer report information in their possession, regardless of whether they personally deem it sensitive or not. No other

---

[8] *See* Fed. Reg., *supra* note 1, at 56,306.

[9] *See id*. (emphasis added).

[10] *See* National Association for Information Destruction, Inc., *Comments on "Disposal of Consumer Report Information"* at 3 (Oct. 20, 2004) (citing §216(a) of FACT Act), *at* http://www.sec.gov.

alternative would seem in line with the goals of the FACT Act.

Second, the Commission should specify the types of monitoring procedures that financial service providers should have in place to ensure that their disposal methods are actually being carried out. The absence of adequate and effective monitoring procedures not only prevents the entity's disposal policies from being reasonable, but it would completely undermine the goal of the FACT Act to protect confidential, sensitive consumer and customer information.[11] Examples of adequate monitoring procedures could include:

(1) Establishing an oversight committee comprised of managers and employees responsible for disposal to carry out the entity's disposal procedures.

(2) Requiring the agents or employees responsible for disposal to make periodic reports (i.e., monthly, quarterly, etc.) to the oversight committee, if any, or to management detailing the amount and type of information that was disposed.

(3) Requiring at least one manager to physically oversee the disposal each period and report to the oversight committee, if any, or to management about the amount and type of information that was disposed.

Third, the Commission should specify what penalties, if any, covered entities will be subject to should their disposal measures be deemed unreasonable. The Commission should establish a clear deadline for the implementation of disposal policies and procedures, and monitor compliance by requiring covered entities to submit reports of their respective plans by the deadline. These reports should include a detailed description of the entity's disposal policies, its choice of disposal method(s), and its procedures for monitoring compliance with those policies and procedures. Should the Commission determine that an entity's proposed policies and procedures are unreasonable,

[11] *See* Fair and Accurate Credit Transactions Act of 2003, H.R. 2622, 108th Cong. (2003) (providing legislative history of FACT Act).

the Commission should promptly notify the entity and provide some type of appeal process. Further, the Commission should allow these reports to be submitted electronically to defray mailing costs. Finally, failure to submit such reports should result in a fine or other sanction that will increase each day, week, month, etc. until the entity complies.

In sum, while the Commission's proposed reasonableness standard is advantageous in its flexibility, it remains inadequate because of its potential to create excess confusion and lead some covered entities to expend unnecessary funds on compliance. I urge the Commission to consider my recommendations for making the standard more stringent while not sacrificing any of its flexibility.

2. The Definition of "Disposal"

In the proposed definition of disposal, the use of the word "abandonment" is unclear. In its present form, the definition states: "the discarding *or abandonment* of consumer report information, as well as the sale, donation, or transfer of any medium . . . upon which consumer report information is stored."[12] On the one hand, it has the same meaning as the word "discard" – by discarding my trash, for example, I am essentially abandoning it. It follows that if the term "abandonment" as used here has the same sense as "discard," which is the word that immediately precedes it in the definition, the definition is redundant. If this is indeed the case, I recommend that the Commission delete the word entirely from the definition.

On the other hand, however, the reality is that the term "abandonment" implies more severe consequences than just throwing out the trash. When I read or hear the word abandonment, I think of abandoned buildings that were vacated and left to rot. So, when I saw the word used here, it naturally gave rise to a concern that a financial service provider could just up and vacate its business operations and leave my personal and financial information sitting on a computer somewhere that anyone could find. Therefore, if the term as used here means something other than "discard," it is dangerous. If this is the case, I encourage the Commission to specify exactly, by example or otherwise, what it means by "abandonment" in this context.

[12] *See* Fed. Reg., *supra* note 1, at 56,305.

Clarification is further needed in terms of what actually constitutes disposal of consumer report information. I recognize and appreciate the Commission's inclusion of the "sale, donation or transfer of any medium . . . upon which consumer report information is stored" within the ambit of conduct that constitutes disposal. However, I do not understand how consumer report information on a computer is disposed of when the computer is sold, donated or transferred, but the information itself is *not* disposed of when it is permanently sold, donated or transferred. In both instances, the financial service provider that originally held the consumer report information permanently discarded it by somehow giving it to someone else. It is unclear why the information must first be on a computer (or other medium) before it will be considered disposed of. I think if the financial service provider is selling, donating or transferring the consumer report information itself, they do not do so with the intention of getting it back. Therefore, the financial service provider is disposing of the information and should be subject to its policies and procedures to ensure that the disposal is proper. In light of these concerns, I urge the Commission to modify the definition of disposal as follows:

> "The permanent discarding of consumer report information by itself, by the sale, donation or transfer to third parties, or by the sale, donation or transfer of any medium, including computer equipment, upon which consumer report information is stored."

In sum, the definition of disposal in its present form is unclear and creates confusion in terms of when consumer report information must be properly disposed of under this rule. I urge the Commission to reconsider the definition in light of the above concerns, and to use my suggested definition as a guide.

3. Definition of "Business Purpose"

The proposed rule lists the financial service providers who might possess consumer report information for valid business purposes,[13] but the Commission has failed to clarify what those valid business purposes are. The

[13] *See id.*, at 56,306, n.17.

Commission states that "a business purpose" includes "all business reasons for which a covered entity may possess or maintain consumer report information,"[14] but provides no examples of what those business purposes might be. Moreover, the Commission states that it views a "business purpose" to be broader than the "permissible purposes" provided by the Fair Credit Reporting Act ("FCRA"),[15] but specifies no limits or provides no examples of what would *not* constitute a valid business purpose.

Section 1681b of FCRA contains the permissible purposes of consumer report information, but it does not specify whether such purposes also constitute valid business purposes. By declaring that acceptable business purposes are broader than the permissible purposes, however, the Commission seems to incorporate the permissible purposes into the purview of valid business purposes. The Commission must be more specific and clearly delineate its position in this regard for two reasons. First, if a covered entity possesses the consumer report information for a reason other than one listed as a permissible purpose in §1681b, that entity is entitled to know whether it is in violation of the Commission's rule. If the Commission fails to more clearly define "business purpose" or specify the limits on what actually constitutes a valid business purpose, it will create confusion and uncertainty among these covered entities and could result in such entities expending unnecessary funds on compliance.

Second, because covered entities need to know when their possession of consumer report information will not generate unnecessary liability, it is imperative that the Commission establish limits, by example or otherwise, that demonstrate what is or is not a valid business purpose. If the permissible purposes for consumer report information are included, then the Commission should say so and then describe how a business purpose goes further and provides covered entities with more flexibility (if that is what it is) to possess the information. If the Commission does not intend to include the permissible purposes in the ambit of what constitutes a valid business purpose, this should also be clearly stated. The Commission should then provide more details on how a business purpose differs from the

---

[14] *See id*.

[15] *See* 15 U.S.C. § 1681b.

permissible purposes delineated in FCRA, and explain that covered entities will not be in compliance with the final rule if they adhere only to the permissible purposes.

Finally, in connection with my comments on the proposed "reasonable measures" standard, because Congress intended that all information contained in or derived from consumer reports be properly disposed of, it makes no sense to exclude those entities that possess consumer report information for reasons other than "valid business purposes." The information possessed by such entities is just as susceptible to identity theft, and should therefore not be considered as less important in terms of the protection it receives. I realize the Commission does not have jurisdiction over every possible entity that might possess consumer report information. The Commission should, however, specify that no entity under its authority may dispose of its consumer report information without adhering to this rule.

4. Definition of "Consumer Report Information"

The Commission defines "consumer report information" as "any record about an individual . . . that is a consumer report or is derived from a consumer report."[16] The definition is over-broad in that it includes consumer information that is already publicly available. For example, because consumer reports contain information relating to one's credit worthiness, such reports will include information like one's history of bankruptcy, which could easily be public information if any part of the bankruptcy proceedings took place in a court open to the public. Moreover, consumer reports also contain information pertaining to one's "character [or] general reputation,"[17] which is generally not secret information that no other member of the public could know.

If the goal of both the disposal rule and the Commission's safeguard rule is to protect personal and financial information that might be vulnerable to identity theft or fraud, the goal is completely undermined when such information is already available to the general public.

---

[16] *See* Fed. Reg., *supra* note 1, at 56,305.

[17] *See id*. at n.9 (defining consumer report).

Moreover, by requiring all financial service providers, regardless of size, to include publicly available information in their disposal policies and procedures, the Commission imposes an unnecessary and excessive burden. Financial service providers have limited resources and should not be required to expend those resources on protecting unprotectable information. For these reasons, I encourage the Commission to implement a general exception to the disposal rule for publicly available information because it is not the type of information that financial service providers should have to account for in their disposal policies and procedures.

Finally, while I appreciate that the Commission believes covered entities subject to the safeguard rule have already addressed the disposal of *customer* records when creating their safeguard policies and procedures,[18] the Commission should either discuss in more detail how these covered entities plan to dispose of customer information, or make a more concerted effort to determine whether the covered entities have really done so. One reason for my concern is that the Commission relies on these entities to utilize similar methods for implementing policies and procedures to dispose of consumer report information, but it has not stated with any certainty that the safeguard policies and procedures followed by these covered entities actually work. As an investor, I need more assurance that both my customer information and my consumer report information will not fall into the hands of identity thieves. The Commission's mere belief that the covered entities have all sufficiently adhered to the requirements of the safeguard rule, without more definitive proof, is not good enough.

A second reason for my concern stems from the fact that the Commission models its ambiguous "reasonable measures" standard for disposing of consumer report information after the "reasonable design" standard required under the safeguard rule to safeguard customer information.[19] By requiring financial service providers to

[18] *See id*. at 56,306.

[19] *See* 17 C.F.R. 248.30 (requiring safeguard procedures to be "reasonably designed" to insure security and confidentiality of customer records and information, and protect against unauthorized access to or use of customer

take reasonable measures to dispose of consumer report information, the Commission hopes to "harmonize" these measures with the reasonable design of the entity's safeguard policy.[20] However, if the Commission cannot say with any certainty that the safeguard policies and procedures supposedly in place at the covered entities are adequate or effective, then it does not seem possible that the reasonable measures taken by that entity to dispose of consumer report information will do any better. Thus, while a covered entity can comply with the proposed disposal rule by applying its safeguard policies and procedures, and linking its methods of disposing of consumer report information with those it uses to safeguard its customer information,[21] it will be pointless if the customer safeguard policies either are not in place or do not work.

In sum, while I commend the Commission for utilizing a definition for consumer report information that is practical, the definition remains lacking in specificity as to what exactly it encompasses. The Commission can address this problem by excepting publicly available consumer information from the information that must be properly disposed of under this rule. As for the remaining consumer report information, however, it is imperative that the Commission do a better job of establishing whether the existing safeguard policies of the covered entities actually work.

B. Policies & Procedures to Dispose of Consumer Report Information & Safeguard Customer Information Should Be in Writing

I agree with the Commission's proposal that all financial service providers subject to the rule should be

---

records or information that could result in substantial harm or inconvenience to any customer).

[20] *See* Fed. Reg., *supra* note 1, at 56,306.

[21] *See id*. ("[A] covered entity could comply with the proposed disposal rule by applying its policies and procedures under the safeguard rule, including methods for the proper disposal of customer information, to consumer report information or any compilation of that information.").

required to put their policies and procedures for the disposal of consumer report information, and their policies and procedures for safeguarding customer information, in writing. My reasons are as follows. First, if the policies and procedures are in writing, they will provide more substantive guidance to the employees or third parties responsible for disposing of the consumer report information or safeguarding customer information. The employees or third parties will actually have documentation of what is or is not to be disposed of (or safeguarded), and would no longer be forced to rely on custom or word of mouth.

Second, written policies and procedures are more difficult to change. The chances are good that no financial service provider will conduct its business ten years from now in the exact same way it does today. The Commission itself recognizes that the needs and resources of financial service providers under its authority will change over time. This recognition is evidenced by the Commission's flexible reasonableness standard. By putting both the disposal and safeguard policies and procedures in writing, the financial service provider can grow, expand its services, become more specialized, or change management and the policies and procedures will endure.

Third, written policies and procedures would better enable the Commission to provide sufficient oversight and compliance reviews. As with the guidance that written policies and procedures would provide to employees, the same holds true for the Commission's examiners. This is evidenced by the Commission's own inability to adequately and effectively oversee compliance with its safeguard rule. Written documentation of a particular entity's disposal policies, for example, would allow the examiners to more easily determine the entity's level of compliance with the Commission's rules, and more readily identify potential problem areas, if any, in the entity's disposal procedures. Thus, it appears that if written policies and procedures were not imperative, the Commission would not propose to amend its safeguard rule to require it.

C. Commission Should Modify Existing Safeguard Rule to Increase Specificity on How Customer Information Should Be Protected

The Commission proposes to amend the existing safeguard rule to include a more specific description of the elements that covered entities must include in their policies and procedures for safeguarding customer information.[22] I agree with the Commission that certain elements are needed in a covered entity's policies and procedures if that entity is to adequately protect its customers' personal and financial information. Furthermore, I agree with the Commission that the Federal Trade Commission's ("FTC") safeguard rule serves as a good model of what the Commission itself can do to improve its own safeguard policy.[23]

Under the FTC's safeguard rule, financial institutions subject to the rule must adopt "a written information security program [that is] 'appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.'"[24] In order for an institution's safeguard policies to be sufficient, that institution must include certain elements, including an identification of reasonably foreseeable internal and external risks that are most likely to pose a threat to the institution's customer information.[25] The Commission seeks comment on whether its own safeguard rule should impose a similar requirement and I suggest that it should.

First, the financial institutions under the authority of the Commission do not necessarily have more complex business operations than those under the jurisdiction of the FTC. Therefore, to keep the Commission's safeguard rule ambiguous just to remain "flexible" is senseless and in some ways, discriminatory. After all, if one set of financial institutions is subject to a more stringent safeguard standard while the other set is not, questions will arise as to the usefulness of a safeguard standard at all. In other words, utilizing two different standards to supposedly protect the same type of information makes it seem like those institutions under the Commission's

---

[22] *See* Fed. Reg., *supra* note 1, at 56,308.

[23] *See id*.

[24] *See id*. (citing 16 C.F.R. § 314.3(a)).

[25] *See id*.

authority are somehow more careful or accurate in protecting their customer information when in fact, they may be the same or worse. It follows that if the Commission believes the FTC's safeguard rule allows for more specificity without sacrificing flexibility, then the Commission should amend its existing safeguard rule to impose the same requirements as the FTC.

Second, if the goal of the safeguard rule is to protect non-public customer information to the best extent possible, then the Commission should not be shy about imposing more specific standards on the financial institutions under its authority. Those entities will want increased specificity so they know not only what they must protect, but also so they know when they can and cannot be held liable. By requiring covered entities to identify potential internal and external risks, for example, the Commission not only encourages those entities to become more aware of the possible threats to their customer information, but it simultaneously puts those entities on alert as to a potential subject of liability if they fail to adhere.

In sum, I encourage the Commission to modify its existing safeguard rule to include more specific elements that covered entities must include in their policies and procedures for safeguarding their customer information. Increased specificity is necessary because it will provide covered entities with a clearer understanding of how they must protect customer information. Furthermore, greater specificity is particularly important in light of the Commission's intent to make its disposal rule consistent with its safeguard rule.

IV. Conclusion

Identity theft is a serious recurring problem in the United States. By enacting § 216 of the FACT Act, Congress recognized the necessity of increased and immediate protection for personal and financial consumer information. I commend the Commission for carrying out its duties under §216 and creating a rule that will provide substantially greater protection for unwary consumers.

I thank the Commission for this opportunity to comment, and respectfully request that the Commission consider the suggestions I have made throughout this

comment. I believe they will aid the Commission in furthering the goals of §216 by reducing the potential for identity theft in a cost-efficient and effective manner.

Respectfully Submitted,

Cheryl A. Tedder