



September 18, 2006

Donald S. Clark, Secretary  
Federal Trade Commission  
Office of the Secretary  
Room H-135 (Annex M)  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Re: The Red Flags Rule, Project No. R611019

Dear Mr. Clark:

ChoicePoint Inc. (“ChoicePoint”) appreciates the opportunity to comment on the proposed rule regarding “Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003” (the “Proposed Rule”).<sup>1</sup> ChoicePoint is a publicly-traded company that, through its subsidiaries, offers technology and information-based products and services to help businesses, government agencies, and nonprofit organizations analyze data and make decisions to reduce fraud and mitigate economic and physical risk. Our Bridger Insight™ suite of products, for example, is used by a majority of the 25 largest banks, as well as thousands of other businesses, to meet certain Patriot Act, Office of Foreign Asset Control, and Bank Secrecy Act obligations, including identity verification requirements.<sup>2</sup>

We believe that the Proposed Rule provides a strong basis from which creditors, financial institutions, and certain users of consumer reports can develop programs to combat identity theft. We suggest, however, that the Federal Trade Commission (the “FTC”) and other agencies<sup>3</sup> (collectively, the “Agencies”) make several modifications and clarifications to the Proposed Rule and the accompanying explanatory text (the “Commentary”) described below, in order to more clearly define who is subject to the Proposed Rule, obligations under the Proposed Rule, and related matters. Our comments address the proposed identity theft prevention program, the red flag guidelines, and the address discrepancy reconciliation provisions of the Proposed Rule in turn.

## **I. Identity Theft Prevention Program**

Definition of “financial institution.” As an initial matter, we suggest that the Agencies define the term “financial institution,” given that a number of obligations under the Proposed Rule apply specifically to financial institutions. The intended scope of the

---

<sup>1</sup> 71 Fed. Reg. 40786 (July 18, 2006).

<sup>2</sup> [www.bridgerinsight.choicepoint.com](http://www.bridgerinsight.choicepoint.com).

<sup>3</sup> We are only submitting these comments to the FTC, as we understand that the FTC will share these comments with the other federal agencies participating in this joint rulemaking. *See*, 71 Fed. Reg. 40786.



term “financial institution” is unclear in the Proposed Rule. The proposed definition of “account” appears to draw on the elements of the definition of financial institution used in the Gramm-Leach-Bliley Privacy Regulations (“GLB”).<sup>4</sup> In the Commentary, however, the FTC suggests that the definition of “financial institution” is narrower than that found in GLB because the FTC estimates that only approximately 3,500 financial institutions—state chartered credit unions—are subject to its version of the Proposed Rule.<sup>5</sup> We believe that the FTC is correct to define the term “financial institution” narrowly given the emphasis of Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”) on identity theft and the extension of credit. We suggest for purposes of clarity that a clear and concise definition of financial institution be added to the Proposed Rule—or at least to the FTC’s version of the Proposed Rule—given the wide range of diverse entities subject to FTC’s jurisdiction. If state-chartered credit unions are the only financial institutions subject to the FTC version of the Rule, we suggest that the FTC version of the final rule make this explicit.

Definition of “account.” We also suggest that the Agencies revise the proposed definition of “account.” The reliance of the proposed definition on Section 4k of the Bank Holding Company Act and related sections of the Code of Federal Regulations, in our view, is not helpful in the context of the range of entities subject to FTC jurisdiction. This is particularly true with respect to activities that are “incidental” or “closely related to” financial activities, which can include certain career counselors and travel agencies among others.<sup>6</sup> We believe that the regulations should be tailored to focus on the types of financial accounts prone to identity theft, rather than relying on definitions developed in an entirely different context.

Application to Business Accounts. We suggest that the Proposed Rule be revised so as to only apply to consumer accounts, rather than business accounts. We note that the Fair Credit Reporting Act is a *consumer* protection statute and that a central tenant of the FCRA is that it applies to consumer transactions undertaken for personal, family, or household purposes, not business transactions.<sup>7</sup>

Fictitious Identities. We request that the Agencies consider clarifying the extent to which creditors and financial institutions are required as part of their identity theft prevention programs to prevent the establishment of accounts on the basis of fictitious identities (other than a “doing business as” construct or other legitimate means), as opposed to an identity of a real person or entity misappropriated by means of identity theft. The Commentary suggests that such a fictitious identity would be beyond the scope of the Proposed Rule<sup>8</sup> despite the fact that such bogus accounts may often trigger

---

<sup>4</sup> 16 C.F.R. § 313.3(k)(1).

<sup>5</sup> 71 CFR 40800, n. 44 (“Under the FCRA, the only financial institutions over which the FTC has jurisdiction are state chartered credit unions.”)

<sup>6</sup> 16 C.F.R. § 313.3(k)(2)(iv) & (ix).

<sup>7</sup> See, e.g., FCRA § 603(d) (definition of “consumer report”).

<sup>8</sup> 71 Fed. Reg. 40790, Item 5. (“In other words, the Red Flags identified by the Agencies must be indicators of ‘the possible existence’ of a ‘fraud committed or attempted using the identifying information of another person without authority.’”)



red flags similar to those prompted by identity theft and could have an adverse impact on safety or soundness of financial institutions.

“Precursors” to Identity Theft. The Commentary suggests that creditors and financial institutions would have obligations under the Proposed Rule to act with respect to what the Agencies refer to as “precursors” to identity theft.<sup>9</sup> In this respect, the Agencies reference phishing schemes as an example of such a precursor. Phishing schemes, while certainly devices for fraud and identity theft, typically appear to be perpetrated by fraudulent actors directly against consumers. The organizations whom the fraudulent actors impersonate customarily are not directly involved in these transactions and may not know for some time that their customers are being victimized. As such, it is unclear how the Agencies anticipate that creditors and financial institutions will be able to detect or counteract phishing schemes through application of the red flag guidelines. Additional clarification on this point would be appreciated.

Safety and Soundness. We believe that the Proposed Rule would be improved if the Agencies would clarify how “safety and soundness” considerations impact the application of the Proposed Rule. Clearly, an institution’s safety and soundness might be harmed as a result of an identity theft incident or incidents and such an outcome may be an additional reason for a company to establish an identity theft prevention program. It is less clear, however, how safety and soundness considerations are relevant to the actual content of the identity theft prevention program. Clarification of this point by the Agencies would be appreciated.

Service Providers. The Agencies sought public comment regarding whether service providers should be permitted to implement an Identity Theft Prevention Program that differs from the programs of the individual financial institution or creditor to whom it is providing services.<sup>10</sup> In our view, the final rule should give financial institutions and their service providers this flexibility. The important consideration is that an effective identity theft prevention program is in place and being complied with. In the case of a service provider that provides services for multiple financial institutions and/or creditors, a requirement that the service provider must be identical to the program of each financial institution and/or creditor could prove ultimately unworkable given the diverse number, sizes, and sophistication of the millions of creditors and financial institutions potentially subject to the Proposed Rule. As such, we believe it would be preferable for the final rule to provide flexibility on this point, so that the creditor or financial institution and its service provider can agree on the most effective outcome.

Supervisory Guidance. The Commentary indicates that creditors and financial institutions have an obligation to incorporate “applicable supervisory guidance” into their identity theft prevention programs.<sup>11</sup> We suggest that the Agencies clarify in the final rule or its commentary that “applicable guidance” is guidance issued by the Agency

---

<sup>9</sup> 71 Fed. Reg. 40790.

<sup>10</sup> 71 Fed. Reg. 40793.

<sup>11</sup> 71 Fed. Reg. 40791.



responsible for oversight of the particular creditor or financial institution and that it is not necessary for financial institutions or creditors to monitor all of the Agencies to determine whether they have issued additional guidance.

Independent Assessment of Third Party Software. We appreciate that the Agencies have recognized the value to creditors and financial institutions from the use of computer-based products designed to assist them as an aid to decision making in identifying their customers and preventing fraud, including identity theft.<sup>12</sup> ChoicePoint’s Bridger Insight suite of products, as noted above, is used by a majority of the 25 largest banks, as well as thousands of other businesses, to assist them in meeting certain Patriot Act, Office of Foreign Asset Control, and Bank Secrecy Act obligations, including identity verification requirements.<sup>13</sup>

In a statement in the Commentary, the Agencies “note” that creditors and financial institutions “must independently assess whether such programs meet the requirements of the red flag regulations and the red flag guidelines and should not rely solely on the representations of the third party.”<sup>14</sup> While we generally agree with this position, we recommend the addition of a statement clarifying that the level of due diligence required is unique to each institution as a function of risk. The assessment should be deemed sufficient if it enables the creditor or financial institution to form a reasonable belief that the software program adequately supports the institution’s identity theft prevention program.<sup>15</sup> We note that it is not the software program that must “meet” the regulations and guidelines, but rather the creditors or financial institutions that are subject to the regulations; a software program is a tool to assist financial institutions and creditors to meet their obligations.

## II. Red-Flag Guidelines

We believe that the Agencies have successfully identified a number of “red flags” which could help financial institutions or creditors identify instances of identity theft. We suggest, however, that the Agencies revise the specific red flags in order to focus primarily on the indicia of identity theft, rather than appearing to prescribe particular steps that a financial institution or creditor must undertake.

We believe that the red flag guidelines are on point to the extent that they identify factors that may be indicative of identity theft, such as falsified or inconsistent information. If the goal, for example, is to have financial institutions and creditors take steps to verify—either directly or through a third party—the social security number,

---

<sup>12</sup> *Id.*

<sup>13</sup> [www.bridgerinsight.choicepoint.com](http://www.bridgerinsight.choicepoint.com).

<sup>14</sup> 71 Fed. Reg. 40791.

<sup>15</sup> As the Agencies properly recognize, the nature of the identity theft prevention program will vary depending upon a number of factors including the “size and complexity of the financial institution or creditor and the nature and scope of its activities.” *See, e.g.*, Proposed 16 C.F.R. § 681.2(c)(1); *See also*, 71 Fed. Reg. 40800, n. 46 and accompanying text (distinguishing between “high risk” and “low risk” financial institutions and creditors).



address, and telephone number supplied on an application then this should be stated as the action item, rather than suggesting, as the Agencies do in proposed red flag number 12, that it is necessary to run these data elements against their entire customer base to look for duplication.<sup>16</sup> Such particularity, in our view, is unnecessary and may prove counterproductive, prompting financial institutions and creditors to institute such a monitoring program because it is referenced in the guidelines, even if it is impractical or not beneficial in the context of that creditor or financial institution.<sup>17</sup>

We also request that the Agencies emphasize in the final rule that these red flag guidelines have been developed with creditors and financial institutions in mind and that while particular red flags may be relevant in other identity-theft related contexts, the Appendix<sup>18</sup> should not be viewed as a universally applicable identity theft prevention program. We also believe that the Agencies are correct to point out that not all red flags that are identified in the Appendix may be applicable to all accounts or suggest identity theft in all contexts.<sup>19</sup> We suggest that the Agencies emphasize in the final rule that the proposed red flag guidelines are intended to be indicative of what a financial institution or creditor may include in its identity theft prevention program, but that it would not constitute a violation of the regulations should a financial institution or creditor elect not to include a particular red flag proposed by the Agencies or fail to implement a red flag precisely as the Agencies have characterized it.

### III. Address Discrepancy Regulations

#### Scope of the Provision

Our principal concern with respect to the address discrepancy reconciliation provisions of the Proposed Rule is that the black letter of the proposed rule itself—§681.1 in the FTC version of the Proposed Rule—does not appear to be consistent with the way in which the operation of the provision is discussed in the Commentary.

Specifically, while the Commentary—as well as Section 315 of the FACT Act—discusses the address discrepancy requirements in connection with nationwide consumer reporting agencies as defined in FCRA § 603(p) (the “603(p)s”); the text of the Proposed Rule itself refers to consumer reporting agencies more broadly, not the 603(p)s specifically. We request that the Agencies clarify—through specific references to nationwide consumer reporting agencies as defined in § 603(p) as appropriate—that the

---

<sup>16</sup> See, e.g., 71 Fed. Reg. 40825 (“12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.”)

<sup>17</sup> In the case of proposed red flag number 12, we question the utility of comparing application information to the information of other applicants or customers. It is not atypical for an individual or entity to have multiple accounts; therefore such a comparison could be expected to consistently produce a high number of false positives.

<sup>18</sup> The Appendix is designated as Appendix A in the FTC version and Appendix J in the versions of the Proposed Rule issued by the other Agencies.

<sup>19</sup> 71 Fed. Reg. 40794.



requirements of this section involve communications to and from 603(p)s only, not all consumer reporting agencies.

In addition, we suggest that the Proposed Rule be revised to more clearly state whether users are obligated to comply with this section when they obtain a credit report originated by the 603(p)s but provided through a reseller.

We also suggest that the Proposed Rule be clarified with respect to the reporting of corrected addresses by users to the 603(p)s. We suggest that the final rule clarify that users of consumer reports be required to send any required address corrections directly to the 603(p)s, rather than through resellers. This outcome appears to be contemplated by the proposed §681.1(d)(1)(3) requirement that addresses be furnished by the user to the consumer reporting agency from which the address discrepancy notice is obtained, but clarification of this point would be beneficial.

We also believe that the clarity of the Proposed Rule would be increased if the Rule or the Commentary included explicit statements that a user of a consumer report has no obligation to furnish a corrected address to a 603(p) unless it regularly and in the ordinary course of business furnishes data to the 603(p), as well as a statement that if employers, landlords, or other report users do not hire or otherwise do business with a consumer whose report was the subject of the address discrepancy, there is no obligation to report a corrected address. Both of these points appear to be implicit in the formulation of factors in § 681.1(d), however, users of consumer reports may find explicit statements to this effect helpful in understanding their obligations in this area.

Use of third party sources for the verification of identity and resolution of address discrepancies

We appreciate the Agencies' recognition in the Proposed Rule that use of information from third party sources is an appropriate means by which a user of consumer reports can meet its obligations under the address discrepancy provisions of the Proposed Rule.<sup>20</sup> We urge the Agencies to retain this flexibility regarding the use of third party information sources for verification purposes in the final rule.

Sincerely,

ChoicePoint Inc.

---

<sup>20</sup> 71 Fed. Reg. 40796; Proposed Rule § 681.1(d)(2)(iii).