



June 2, 2004

Federal Trade Commission
P.O. Box 1030
Merrifield, VA. 22116-1030

Subject: FACTA Identity Theft Rule, Matter No. R411011

Dear Sir or Madam:

Boeing Employees' Credit Union (BECU) appreciates the opportunity to comment on the FACTA proposal on identity theft. BECU is a state-chartered federally insured credit union with assets of \$4.6 billion and a membership base of over 350,000.

There were a number of questions that you wanted addressed. We will answer each one in the order presented.

A. Questions relating to the definition of identity theft.

1. Does the term "identity theft" as defined by the Act need further definition?

The definition is very general. It should include that identity theft only applies to fraud initiated by a person other than the consumer, without actual or implied authority to initiate the transaction and from which the consumer receives no benefit. It would not apply to any transaction that was initiated with fraudulent intent by the consumer or any other person acting in concert with the consumer.

2. Should the FTC define the term "identifying information" to have the same meaning as "means of identification" in U.S.C. 1028(d)(4)?

We agree with this definition. It includes all of the typical information used for identification.

3. Should the FTC add the element of "attempt" to the definition of the term "identity theft"?

We agree with this, but it should describe the result of the attempt (e.g. resulting in the unauthorized inquiry on a consumer's credit report). Currently, it is only possible to have inquiries hidden and not removed by writing a letter to the CRAs. We recommend FTC develop an easier process for the consumer and the information furnishers to have unauthorized inquiries removed.

4. Should the FTC add the element that a person's identifying information must be used without such person's knowledge to the definition of the term "identity theft"?

Yes, in our opinion, FTC needs to specifically define who is entitled to this protection. Identity theft only applies to fraud initiated by a person other than the consumer, without actual or implied authority to initiate the transaction.

5. Should the FTC add the element that a person's identifying information must be used without such person's lawful authority to the definition of "identity theft"?

Yes, same response as number A4.

1. Are there additional elements that FTC should add to the definition of the term "identity theft?"

See response in A1.

A. Questions relating to the definition of identity theft report.

1. Does the term "identity theft report" as defined by the Act need further definition?

We believe this should be defined to state exactly what needs to be in the report. It should be of adequate content that the financial institution could pursue the fraudulent amount. The consumer needs to be cooperative to provide information to the satisfaction of the financial institution. The financial institution must be informed immediately upon consumer knowledge of the event so that further losses can be prevented. If not, then the consumer should be held liable in some manner.

2. Should FTC define what is an "appropriate law enforcement agency?"

The examples listed in the proposal appropriate Federal, State, or local law enforcement agency, including U.S. Postal Inspection Service, or such other government agency seems adequate.

3. To deter abuse of the credit reporting system, the Act requires that an identity theft report be subject to criminal penalties for false filing and allows consumer reporting agencies and information furnishers to reject or block or continue furnishing information. How likely is it that these safeguards will deter abuse of the credit reporting system? Are these safeguards less likely to deter abuse when automated systems are available to generate reports? Are there alternate ways to deter abuse other than what has been proposed?

We do not agree with the automated method of reporting identity theft. Allowing the reporting to be a faceless transaction with zero law enforcement involvement makes it extremely convenient for someone to falsify a report. In our opinion, to qualify for these protections, the consumers must provide adequate proof of fraud in person. We are all for making it easy for the victim to report, but there should be more substance to this plan. Additionally, law enforcement agencies should be willing/obligated to pursue.

4. Are the examples provided by FTC of when it may or may not be reasonable for information furnishers or consumer reporting agencies to request additional information or documentation useful? Are there alternate examples that would be more useful?

We feel it would be more appropriate to provide guidelines of how we can determine if it falls within the law. Provide us the ability to reject a customer's claim if not adequately proven.

B. Questions relating to the duration of active duty alerts.

1. Should FTC maintain the duration of the active duty alert at the minimum statutorily determined length of 12 months as proposed?

We agree with the proposal. We believe that 12 months should adequately cover the period that the majority of service members will be deployed.

C. Questions relating to appropriate proof of identity.

1. Should FTC set specific standards for what constitutes appropriate proof of identity?

We agree with the FTC. The information necessary to prove that a consumer is who he/she claims could be substantially more burdensome for a consumer to produce and might result in delays or even failure to obtain the requested service if the consumer reporting agency (CRA) is unable to identify the consumer. To receive a consumer file match, the examples that were provided in the proposal seem appropriate (proof of full name, any other name used, full address, social security number and date of birth).

2. Are the examples of information that might be required by CRAs appropriate or inappropriate? Is there alternate information that should be used for examples?

We agree with the examples (listed in D1 above) that give guidelines to consumers on what they are required to provide to qualify for these protections.

3. Has FTC adequately balanced the harm that might arise from the consumer being misidentified and the harm arising from delays in, or potentially failure to provide the consumers' requests due to greater levels of scrutiny?

In our opinion, it appears the consequences for misusing the blocking of fraudulent information on consumer reports are equal to or outweigh the benefits for abusing it. We recommend further work be done by the FTC.

We have the following recommendations on other parts of the proposal:

- a. Identity theft report: On the proposed requirement that would have the consumer describe the theft with as much specificity as possible, we recommend the FTC develop an affidavit that the consumer attests they did not participate in or benefit from the transaction and a binding pledge that they, as the victim, will support the prosecution of the criminal, if we identify one.
- b. When allowing information furnishers or CRAs to request additional information or documentation to help determine the validity of the alleged identity theft, we recommend extending the amount of time to request additional information from the consumer from 5 business days to 15 business days. Depending on the amount of cases the financial institution has, 5 days could be burdensome.
- c. If a consumer has filed a false identity theft report, we recommend punitive penalties. It's not clear on whose responsibility it is to prove the report is false or if it is the consumer's responsibility to prove it's accurate.

Thank you for the opportunity to respond on the proposal. We look forward to the final outcome.

Sincerely,



Gary J. Oakland
President and CEO



Joe Brancucci
Vice President of Lending