



UNITED STATES OF AMERICA  
**FEDERAL TRADE COMMISSION**  
WASHINGTON, D.C. 20580

**Registration Web Site for the FACTA Credit Report Accuracy Study  
Privacy Impact Assessment**

**February 2008**

## 1 INTRODUCTION

The Federal Trade Commission (FTC) is doing in a long-term study on the accuracy of information contained in consumer credit reports (background below). In the second pilot phase of this study, researchers at the University of Missouri (“University”), which is serving as a consultant to the FTC for this phase, will be creating and using a Web site to register individuals who volunteer to participate in the study. As required by the E-Government Act of 2002, the FTC is posting this privacy impact assessment (PIA) to explain to the public what information the Web site will collect from individuals, why it is being collected, and how it will be safeguarded to protect its privacy.

## BACKGROUND

In December 2006, the FTC issued a report to Congress under Section 319 of the Fair and Accurate Credit Transactions Act of 2003, which requires the FTC to study the accuracy and completeness of information in consumers’ credit reports and to consider methods for improving the accuracy and completeness of such information.<sup>1</sup> The requirement includes five interim reports (every two years from December 2004) and a final report in 2014. The December 2006 Report is the second interim report.

The first report was issued in December 2004 and outlined a pilot study for testing a potential methodology for a nationwide survey. In the pilot study, randomly selected consumers reviewed their credit reports with an expert to identify potential errors, and then disputed potential errors that the expert believed could have a non-trivial effect on their credit standing. Based upon the results, the FTC is undertaking a follow-up pilot study in order to help improve the design for a nationwide survey that can accurately assess the credit reporting process.<sup>2</sup>

The Commission’s goal is to achieve a nationwide survey of credit reports that focuses on consumers and their experiences in identifying and disputing errors, is based on a nationally representative sample, uses a reliable method for identifying errors and omissions, and categorizes errors by type and seriousness in terms of potential consumer harm.

## OVERVIEW

As explained further below, the purpose of the Web site created for the FTC’s second pilot study is three-fold: (1) to determine that the individual is eligible to participate (e.g., 21 or older); (2) to confirm that the individual knows and consents to the terms of participation (e.g.,

---

<sup>1</sup> Copies of the Commission’s report are available from the FTC’s Web site at <http://www.ftc.gov/opa/2006/12/fyi0679.shtm> and also from the FTC’s Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

<sup>2</sup> Those who are interested in the overall design of these pilot studies may consult the Federal Register Notice (71 FR 61776 (October 19, 2006)). The same notice is available at the agency’s Web site: <http://www.ftc.gov/os/statutes/fcrajump.shtm>.

to have their credit reports reviewed for accuracy by the FTC's research team), and (3) to register those individuals who qualify and consent. The study group for this second pilot is expected to comprise no more than approximately 100 to 120 individuals.<sup>3</sup>

Participation in the FTC's pilot study is completely voluntary, and there is no consequence for not participating. Participants in the study will provide very limited personal information to the Web site: name; address; telephone number; and e-mail address. In return, the individual will receive a unique login ID identifying the individual as a study participant, a voucher number associated with the study, and a self-assigned password. The individual will be instructed to use this information in order to log in on a separate Web site ([www.myfico.com](http://www.myfico.com)) that is already operated by the Fair Isaac Corporation (FICO) in cooperation with the three major national credit reporting agencies, Equifax, Experian, and TransUnion. (Neither the FTC, nor its research team, controls or operates the FICO Web site, which is funded and maintained by private sources.) Through that Web site, individuals will obtain copies of their personal credit reports and scores for free, and a copy of the participant's credit report information is maintained by the FTC's researchers so that it can be reviewed for accuracy with the participant.

The Web site being created for the FTC's study will not collect or maintain any sensitive identifying information, such as financial account numbers, Social Security numbers, drivers' license numbers, or similarly sensitive information. As explained below regarding security measures and data safeguards, all the information collected by this site will be maintained in a password-protected database in encrypted form

---

<sup>3</sup> This second pilot study, just as the first, is not a statistical study. The pilot studies do not rely on a nationally representative sample of consumers, and no statistical conclusions are drawn. The purpose of these studies is to help improve the design of a national survey.

- C Best time for calling (evenings, mornings, etc.)
- C Email address
- C study code
- C self-assigned password
- C login ID
- C voucher number (all of the latter three to be used at *myFICO.com*)<sup>4</sup>

As noted above, it is anticipated that this information will be collected by the Web site from approximately 100 to 120 individuals.

In addition, the University server for the Web site collects (i.e., preserves) “log” information (IP address, date and time of visit) of individuals who visit the Web site with or without registering for the study; this information is saved for one year. “Cookies” (i.e., small text files placed and stored on the user’s computer by the Web site, which can be used to collect and maintain information about the user’s activities on the Web site) are non-persistent, that is, they will be deleted automatically when the user closes the Web browser by which the information is collected.

No sensitive identifying information ! such as financial account numbers, social security numbers, driver’s license, or similar sensitive information ! is collected or maintained by the Web site.

## **2.2 Why the Information Is Being Collected (Purpose of Collection)**

The purpose(s) of information collection at this Web site all relate to executing the second pilot study; specifically: (1) to determine that the individual is eligible to participate (e.g., 21 or older); (2) to confirm that the individual knows and consents to the terms of participation (e.g., to have their credit reports reviewed for accuracy by the FTC’s research team), and (3) to register those individuals who qualify and consent.

The collected contact information will allow the FTC’s researchers to communicate with study participants. Once the information has been collected by the Web site, the participant will receive an automated email message providing further information on how to register at the separate *myFICO.com* Web site already maintained by Fair Isaac in order to obtain credit reports

---

<sup>4</sup> A password is created by the participant and is entered at the Web site. For security reasons, once a password is entered it is not disclosed (electronically or otherwise) in any communication between consumers and the FTC’s researchers. As explained in Section 2.2, the password and the login ID generated and assigned to the participant are used by that individual to obtain credit reports and scores at *myFICO.com*, which enables similar access to those records by the FTC’s researchers through that Web site. The subsequent review of credit report information in this study follows the same procedures as in the first pilot study. The various forms, formats, and procedures are described in the contractor’s report on the first pilot study. (The contractor’s report is included in its entirety in the December 2006 Report to Congress; <http://www.ftc.gov/opa/2006/12/fyi0679.shtm>.)

and scores at no charge to the participant. The email message provides a login ID (unique to the participant) and a voucher number (also unique to a participant) to be used by the consumer in creating an account at *myFICO.com*. The email does not communicate the self-assigned password that is also to be used in establishing the account. As noted above, the FTC's Web site will collect, i.e., require the participant to enter, a self-assigned password ! a further purpose of which is to enable FTC researchers to obtain duplicate copies of the participants' credit reports and scores through the *myFICO.com* site upon entering a participant's password and login ID. The "study code" is provided (e.g., by a bank or other referring organization) when soliciting customers or others to volunteer for participating in the study. The purpose of the code, which is required to enter the registration Web site, is to ensure that the Web site is used only by such prospective participants,<sup>5</sup> and can also be used by researchers to identify the source of the referral. The University's server collects "log" information automatically for site management purposes.

### **2.3 Intended Use of the Collected Information**

Information collected by the Web site from study participants (name, address, telephone number, and email address) will be used to establish and maintain contact with the participants for the duration of the study. Also, in order to establish the required account at *myFICO.com* to download credit reports, a participant must enter a login ID, self-assigned password, plus a voucher number, all of which will be provided to the participant during the registration process at this Web site. The FTC's researchers will use the same login ID and password to print the participants' (redacted)<sup>6</sup> credit reports, in order to discuss them with those participants.<sup>7</sup> Thus, the login ID is used to relate a participant to his or her credit report information. The distribution and use of study codes (which enable a person to view these screens) are explained in Section 2.6.5.

---

<sup>5</sup> Subsequent screens address a description of the study, qualifications to participate, and a person's consent to participate.

<sup>6</sup> Credit reports are formatted at Fair Isaac so that the digits of any SSN and most of the digits of any account number are suppressed when credit reports are printed through the site *myFICO.com*. (Some digits of financial account numbers are displayed for ease of reference.)

<sup>7</sup> As in the first pilot study, a separate research database contains the information derived from a review of the participants' credit reports. Any personal information derived from the Web site will not be placed in the research database. Nor will any individual consumer data be placed in the research database. Instead, summary information (such as number of credit accounts, outstanding credit balances, credit scores, and numbers and types of errors identified) will be created and used to produce numerical summaries for groups of consumers. A unique identifier is assigned as an alternative to using the SSN for associating credit report information with specific study participants.

## 2.4 Sharing and Disclosure

Personally identifiable information collected by the Web site will be used by the research team and will not be transferred to the FTC or become part of any agency (Government) records. (Likewise, Web site logs maintained by the University are not transferred to the FTC or made any part of FTC records.) Only the aggregate results of the researchers' study (not identifiable by individual participant) will be shared with the FTC. FICO will also not be given access to participant contact information collected through the registration Web site, even though participants themselves will need to submit the login ID, password, and voucher numbers assigned by the registration Web site to establish an account at the FICO Web site and download

---

<sup>8</sup> In the first pilot study, before any credit reports could be drawn, a participant needed to sign and mail back a prepared paper consent form. This process often involved weeks of delay.  
(continued...)

## 2.6 Security Measures and Data Safeguards

Information collected by the Web site is maintained by the contractor (i.e., the University) in a dedicated Oracle database in encrypted form. Access to the database is restricted to database administrators and controlled by password, user domain, and work station ID. The database is maintained with standard protections accorded for commercial applications such as credit card payment, despite the fact that no sensitive personal information (such as SSN, account number or credit card information) is collected by the Web site. All Web site functions are encrypted under “https” (a secure Internet protocol) to protect the consumer against interception of communications.

Although this PIA focuses only on the information collected through the registration Web site, the FTC notes that the procedures for handling credit report data to be obtained by researchers with the participants’ consent (from the FICO Web site) has been scrutinized by the lead contractor’s Independent Review Board for research involving human subjects, and the procedures have received their approval. Overall, and as explained below, the handling and storage of all data for this study overall has been designed to minimize any risk to consumers from illegal hacking or system intrusion.

**2.6.1 Safeguards Rule.** In the course of the study, each participating institution and individual members of the research team will take care to work in conformity with relevant data safeguards, as described in "Financial Institutions and Customer Data: Complying with the Safeguards Rule," see <http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm>. The Fair Isaac Corporation stipulates that it conforms to these practices in its normal business practices and will do so in the handling of consumer information in the course of this study. Fair Isaac gives password-protected participant access to on-line information at the *myFICO.com* site for a period of 35 days after a credit report is downloaded. After 35 days, the down-loaded information is transferred to an archive accessible only by a special service application within the company.

**2.6.2 Employee Management and Training.** All members of the research team are provided with copies of the Safeguards Rule and sign an agreement to adhere to the confidentiality and security requirements of the study. References are checked for any new employees engaged for the study (e.g., telephone recruiters and interviewers). Each member of the research team is provided with detailed descriptions of the data that will be handled in the course of the study (including prototypical credit reports) and will be trained to conform to the research protocols for protecting the consumer against the release or misuse of data. Researchers working for the lead contractor (the University) receive and are certified in human subjects training under guidance of the University’s Independent Review Board for research involving human subjects. Access to any information is limited to persons who have a need to see it.

---

<sup>8</sup>(...continued)

In this second pilot study, the Web site requests that the individual, merely as a backup measure, print out and sign the consent form and mail it in, after completing the electronic registration process.

**2.6.3 Information systems.** Consumer data in hard-copy form, e.g., printed versions of the redacted credit reports, are stored in a secured area – in a locked cabinet and in a (further) locked office. Logs are maintained for files removed for consumer contact.<sup>9</sup> SSNs do not appear in any hard-copy or electronic records maintained by the University. Also, SSNs and all but the last three or four digits of credit account numbers are suppressed in hard copies of credit reports that are mailed to consumers and used by the researchers. A unique identifier is used as a cross-reference between consumer contact information (name, address and phone number) and the information in a credit report. Electronic copies of consumer contact information are kept in separate computer files from those used to record data derived from reviews of the credit reports. The contractor thus maintains background information (such as name and address for contacting the consumer for the credit review) separately from the credit report and demographic data. Password protection is used to limit access to computerized data.

**2.6.4 Data security and consumer confidentiality.** The research team takes care to use secure methods when downloading, transferring, or otherwise electronically communicating any personal data. To enable the consumer to authorize the drawing of credit reports through the secure Web site at *mt*

---

<sup>9</sup> Although the FICO Web site is not covered by this PIA, we note that Social Security numbers will be required by that Web site for participants to be able to access and obtain their credit reports and scores.

<sup>10</sup> The consumer-created password enhances the security of the data. The automated email sent to the participant upon completion of the registration process informs the participant of the login ID and voucher number, and will not include the consumer-created password, all of which the participant will use at the FICO web site when establishing an account and downloading credit reports at that site. Thus, even if the registration email sent to the participant were somehow intercepted, the emailed information would not be enough to access the participant's account at the FICO Web site to obtain that individual's credit report information.

<sup>11</sup> Regarding the contemplated use of referral organizations in the second pilot study, see the FTC's December 2006 Report to Congress (at 5).



participant, without the need for referral organizations to disclose or transfer customer lists or contact information to the research team for recruiting purposes, thereby eliminating the potential risk of loss, theft or misuse of such lists or contact information. Thus, contact information is collected only from those individuals who actually visit the registration Web site and register to participate.

**2.6.6 Handling files with alleged errors.** Files with alleged errors are subject to rescoring by Fair Isaac. Researchers will furnish Fair Isaac with hard copies of files with alleged “corrections” imposed. Before transmitting copies of the “corrected” files to Fair Isaac, researchers will ensure that all identifying information (names, addresses, employer names, etc.)

formal, written request under that Act to ask the FTC for the opportunity to review their records

\_\_\_\_\_ Date:

Marc Groman  
Chief Privacy Officer

\_\_\_\_\_ Date:

Margaret Mech  
Chief Information Security Officer

**Approved:**

\_\_\_\_\_ Date:

Stanley Lowe  
Chief Information Officer