



**Privacy Impact Assessment for the  
Collection Resource System (CRS) and Supporting Systems**

March 12, 2009

Contact Point: Jack Frazier  
System Owner: Richard Fumerelle  
Authors: Bryan Wiler and Lisa Schwartz



## PURPOSE

The privacy provisions of the E-Government Act of 2002 require Federal agencies and their third party service providers to protect the privacy of personal information.

## INTRODUCTION

As a wholly-owned subsidiary of Sallie Mae, Pioneer Credit Recovery operates a flexible, responsive, self-contained company, while enjoying the backing and support of a publicly traded Fortune 500 corporation.

Pioneer Credit Recovery recognizes the importance of protecting the privacy of personal information and uses the Privacy Impact Assessment (PIA) process to identify and address privacy issues in conjunction with this project.

### 1. What information will be collected for the system?

The information that is collected on the system is personal information that is needed to perform debt collection activities. The information collected includes key data elements such as: customer name, address, phone number, date of birth, social security number, place of employment, financial statement information, banking account information, date of death, bankruptcy information and other pertinent information applicable to the collection and processing of debt.

#### Customer Information

Information Type	Source
First name, middle name and last name	Department of Education
Home phone number	Department of Education
Social Security Number (SSN)	Department of Education
Customer's Credit Bureau Report	TransUnion or Experian
Account/Debt related information	Department of Education
Financial assets and liabilities	Customer provided
Employer name, address, phone number, compensation	Department of Education and Customer provided
Named dependants and their SSN	Department of Education
Attorney Information	Department of Education and Customer provided
Co-Borrower Information	Department of Education

**Skip Tracing Information**

<b>Information Type</b>	<b>Source</b>
Demographic data	Fast Data, Experian, Trans Union, Insight, Teletrack, CBC Innovis, Accurint
Customer's name and address	Fast Data, Experian, Trans Union, Insight, Teletrack, CBC Innovis, Accurint
Customer's Social Security Number	Fast Data, Experian, Trans Union, Insight, Teletrack, CBC Innovis, Accurint
Customer's birth date	Fast Data, Experian, Trans Union, Insight, Teletrack, CBC Innovis, Accurint
Customer's employment information	TALX, Fast Data, Experian, TransUnion, Insight, Teletrack, Accurint
Customer's property ownership	Fast Data, Experian, TransUnion, Interactive Data, Insight, Accurint
Customer's nearby, landlords, etc	Fast Data, Insight, Accurint
Customer's incarceration, death, judgment, and lien information	Central Research, Experian, TransUnion, Banko
Customer's bankruptcy information	Banko, Pacer

**2. Why is this information being collected?**

The information that is collected is being used to perform collection activities and support processes for the Department of Education. This includes determining the ability of the debtor to pay the debt, skip tracing analysis, debt payment processing and complying with regulatory requirements.

**3. How will Pioneer Credit Recovery use this information?**

This information is utilized by employees and approved vendors to perform or support collection activities as determined by their job function on behalf of the Department of Education.

**4. Will this information be shared with any other agency or entity? If so, with which agency or agencies/entities?**

Information is shared with service providers in connection with its provision of services directly to Pioneer Credit Recovery in support of the Department of Education Contract. The current providers are:

- Lexis Nexis (Accurint)
- Lexis Nexis (Banko)
- TALX (The Work Number)
- Central Research
- First Data Resources (Fast Data)
- Interactive Data
- Acxiom (Insight)
- Teletrack
- CBC Innovis
- Experian
- Trans Union
- CR Software LLC (CRS)
- Noble Systems Corporation (Noble Dialer)
- E-Commerce Group (Western Union and Speedpay)
- Matrix Printing Solutions
- Pacer
- Iron Mountain

In the event that a new vendor is needed, they are required to adhere to all applicable Sallie Mae corporate policies. All existing or potential new vendors with which customer information is shared go through the Sallie Mae Vendor Risk Management Program.

**5. Describe the notice or opportunities for consent that would be or are provided to individuals about what information is collected and how that information is shared with other organizations?**

The Pioneer Credit Recovery receives information from the Department of Education, Federal Student Aid Debt Management and Collection System (DMCS). As DCMS is the parent system from where Pioneer Credit Recovery receives privacy information, the DCMS warning and privacy disclosure statement below is used:

DISCLOSURE STATEMENT: “The user understands that the Department of Education, its agents and sub-contractors have signed up to meet the requirements of the “PRIVACY ACT of 1974” (as amended). As such, by entering this system, the user hereby verifies that he/she has read the “PRIVACY ACT of 1974” (as amended), that the user understands the requirements of the act, and that the user has no remaining unanswered questions.”

The Pioneer Credit Recovery will not further disclose the information except as defined by the System of Records Notice in the interest of the U.S. Government and the

Department of Education. Pioneer Credit Recovery company privacy policy also restricts the sharing of information.

## **6. How will the information be secured?**

Customer information will be secured using the following physical, operational and logical and vender controls:

### **❖ Physical Controls:**

Pioneer Credit Recovery's Physical Security Program details the implementation, management and administration of physical security at Pioneer Credit.

The internal building layout is designed to separate work areas with different or changing physical security and data security requirements. Sensitive areas such as the Record Storage Rooms, IT Department, Data Center, Accounting offices, Electrical Room, and Telephony Room require special access, controlled by a proximity reader. Access is logged, and invalid access attempts generate alerts to the Pioneer system administrator for investigation.

Our facilities are monitored by Closed Circuit TV (CCTV) 24 hours a day. Monitored areas generally include (but are not limited to) entrances, emergency exits, outside dumpster, backup generator, and sensitive controlled internal locations.

Authorized personnel are issued photo proximity cards which contain electronic access control credentials, providing clearance to controlled areas specific to individual duties. Non-employees (visitors and contractors) may be admitted to facilities subject to local procedures developed by the Facility Department. A written record of all visitors is maintained, visitors are required to provide government issued photo ID, such as a driver's license, for identification purposes. Each visitor is assigned a badge to identify that person as a visitor. This badge is returned when the visitor signs out upon exit. All visitors must enter though a secure entrance and wait in a reception area until escorted within the facility by a Pioneer Credit Recovery employee. Visitors are escorted at all times while on the premises. Visitors not displaying badges or not escorted are subject to challenge and removal from the premises.

All information assets that are considered confidential, sensitive or business critical are, at a minimum, stored in lockable file cabinets which have limited key distribution. File cabinets are locked when not in use and are checked by personnel prior to leaving work at the end of the day. Interior secured areas are set up with either electronic access and/or 5 pin key lock to prevent undetected entry by unauthorized persons.

❖ **Logical Controls:**

Pioneer has developed and maintains standard Network Security and Application Security procedures in compliance with Sallie Mae's Corporate Information Security Policy. These policies are developed based upon ISO-1799 and FISMA standards and specify the following criteria:

- User Access Approval Procedures
- User Authentication Methods
- Password Criteria
- Network Configuration Management Parameters
- Intrusion Detection Systems
- Event Logging and Monitoring

All applicable Linux servers and the file-path are encrypted to ensure appropriate protection of stored customer information within CRS databases and backup storage media. Linux file-path encryption is based on a non-proprietary encryption algorithm. Privileged access to the Linux server is restricted and reviewed on quarterly basis. In addition, a quarterly vulnerability scan is performed using Qualys.

For the CRS Application, all user access is based upon job responsibility and requires management approval. CRS utilizes Microsoft Active Directory for all user access.

In addition to the CRS database, information is also contained in Microsoft Access databases. These databases are located on Microsoft Windows Servers and are secured by Active Directory. In addition to management approval, the network resource owner also approves all access to these databases.

All user access for the Noble dialer is based upon job responsibility and requires management approval. A 256-bit encryption at rest process is in the process being implemented. The targeted implementation date is during the 2nd quarter of 2009. This will provide an additional level of security.

All remote access requires multi-factor authentication utilizing RSA SecurID tokens.

For additional details, please refer to the following documents:

- Sallie Mae Corporate Information Security Policy
- Sallie Mae Network Security Information Security Standards Manual
- Sallie Mae User Access Information Security Standards Manual

❖ **Operational Controls:**

Pioneer has developed and maintains Information Security policies. Procedures are documented to ensure proper controls exist for access management, information asset use and system development life cycle. Job roles are defined to assign responsibility for information security management and ongoing technical design of logical controls.

A security awareness training program and an annual compliance recertification is in place to provide employees with tools and knowledge needed to make good decisions on protecting information assets. Periodic security awareness reminders are also posted.

A pre-employment screening process is in place – including in-depth criminal history checks.

❖ **Vendor Controls:**

A Vendor Risk Assessment Questionnaire (VRAQ) must be completed when the estimated annual spend with the selected vendor is anticipated to be over \$50K. Vendors who are to receive, maintain, process, or otherwise access customers' non-public personal information (NPI), must comply with Sallie Mae's Customer Information Safeguarding Program which includes the completion of the GLBA Classification Questionnaire. The scored GLBA Classification Questionnaire is used as the initiating document for the Security Assessment Framework (SAFe) program. SAFe is used to determine if a potential or actual vendor has adequate controls in place to protect customer NPI.

For additional details, please refer to the following documents:

- Sallie Mae Customer Information Safeguarding Program
- Sallie Mae Corporate Information Security Policy
- Sallie Mae Vendor Risk Management Program

**7. Is a system of records being created or updated with the collection of this information?**

A "System of Records" was created for the Common Services for Borrowers (CSB) Contract. Pioneer Credit Recovery is working under this "System of Records."

The "System of Records" was published in the Federal Register (Volume 71, Number 14/Monday, January 23, 2006/Notices).