Privacy Impact Assessment
For
Sallie Mae Commercial System (SMCS)

Date:
September 11, 2009

Point of contact:
Jonathan E. Kroehler

System Owner:
Jonathan E. Kroehler

Author:
Brian Hynes

Office of
Federal Student Aid

U.S. Department of Education (ED)

Expiration Date: September 1, 2010

1. **System Information. Describe the system** – include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

The Sallie Mae Commercial System (SMCS) services the Federal Student Aid (FSA) Title IV Student Loan Processing environment for all aspects of student loan servicing. Operational capabilities of the system include borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, collection, skip-tracing, claims and correspondence history files. The SMCS communicates with the internal FSA platforms, borrowers, educational institutions, lending institutions, other loan servicers, third-party data providers, consumer reporting agencies, guarantors and government agencies (as permitted by the Federal Privacy Act of 1974). Channels of communication include mail, phone calls, a secure borrower Web site, email and secure data transfer links.

2. **Legal Authority**. **Cite the legal authority to collect and use this data.** What specific legal authorities, arrangements and/or agreements regulate the collection of information?

The SMCS will be acting as a component of the broader ED FSA loans servicing solution, which derives its legal authority to collect and use the information from and about the borrower from §421 et seq. of the Higher Education Act (HEA) of 1965, as amended (20 U.S.C. 1071 et seq.), and the authorities for collecting and using the borrower's Social Security Number (SSN) are §§428B(f) and 484(a)(4) of the HEA (20 U.S.C. 1078-2(f) and 1091(a)(4)) and 31 U.S.C. 7701(b).

3. **Characterization of the Information**. **What elements of Personal Identifiable Information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number, etc.)?** What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (Web site, paper form, online form)? Is the information used to link or cross-reference multiple databases?

The SMCS collects and maintains the following PII data pertaining to borrowers/co-borrowers/co-signors/students:

- Full name.
- Maiden name.
- SSN.
- Driver's license number and state.
- Alien registration number.
- Home street address.
- Work street address.
- Email address.
- Home phone number.
- Work phone number.
- Mobile phone number.
- Date of birth.
- Customer identification number (CIN).
- Loan number.
- Bank account numbers.
- Other borrower information such as: disbursement amount, outstanding loan payment amount, monthly loan payment amount, loan status, forbearance status, deferment status, separation date, grace period, and delinquency status.

The information is obtained from sources such as borrowers, students, co-borrowers, co-signors, educational institutions, lending institutions, other loan servicers, employers, references and external databases (e.g., Directory Assistance, National Change of Address (NCOA), CODE-1, consumer reporting agencies and skip trace vendors).

It is collected via the following channels:

- Phone calls with customer service agents.
- Entries via the Interactive Voice Response (IVR) service.
- Incoming correspondence (e.g., via U.S. mail, email, etc.).
- Entry via the SMCS borrower Web site (www.ed.manageyourloans.com).
- Bulk file transfers from third-party data providers (e.g., Directory Assistance, National Student Clearinghouse (NSC), CODE-1), educational institutions and other loan servicers.
- As required, secure data transmission from ED applications such as the National Student Loan Data System (NSLDS) and the Debt Management Collection System (DMCS).
- Secure data transmission from the U.S. Department of Treasury (Treasury).

The information is used in connection with loan processing and servicing activities, such as identity verification and authentication during online account creation and phone calls, verification between internal databases within the SMCS, and data exchange with external trading partner databases such as:

- Consumer reporting agencies.
- Lending institutions and other loan servicers.
- Directory Assistance.
- NCOA system.
- Educational institutions.

4. **Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity**. Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information is being collected to support the SMCS loan processing and servicing functions such as:

- Loan detail verification.
- Mailing of forms for loan forbearance, deferment and repayment option modifications.
- Mailing/e-mailing of statements of account.
- Mailing of change of address inquiries.
- Identity verification for account management.
- Identification and verification during loan conversion/de-conversion.
- Call scheduling.
- Loan transfer/put/un-put activities.
- Issuance of loan discharge and forgiveness claims and correspondence.
- Maintenance and preparation of loan and account history records and reports.
- Audit and program review planning.
- Internal process optimization.
- Tracking loan borrowers and overpayment debtors.
- Provide information to track refunds/cancellations.
- Transmit loan information to FSA loans central processing platform via ED applications such as NSLDS, DMCS and Conditional Disability Discharge Tracking System (CDDTS).

Identified Privacy Risks and their mitigation measures are discussed in the following.

PII Confidentiality Risks:

- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII during a call with the IVR or a customer service agent via screenshots, access to the customer agent screen or transfer of information from the agent him/herself.
- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII by accessing the SMCS databases.
- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII by tapping into an online account session.
- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII by duplicating a borrower password.
- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII during data transmissions to FSA central loans processing and external databases.

PII Data Integrity Risks:

- The ability of authorized/unauthorized employees and unauthorized non-employees to alter PII by accessing the SMCS databases.
- PII data entry errors to the databases.

Key Risk Mitigation Measures:

- All SMCS personnel are required to obtain government security clearance and complete ED's initial Security Training and Awareness course as well as periodic refresher training.
- All SMCS infrastructure is located in facilities that leverage appropriate environmental controls.
- The SMCS maintains appropriate systems for redundancy and failover.
- The SMCS maintains personnel and facility security measures.
- All staff members with SMCS access who work in shared workspaces will have screen filters installed for all workstations processing PII and ED information.
- Borrower account access via the secure Web site requires authentication via a User ID (UID) and account password.
- Borrower account access via the IVR or customer service call centers requires appropriate authentication.
- PII and ED loan data and database access requires properly documented authorization and is electronically implemented.
- PII and ED loan databases are maintained according to the appropriate NIST specifications and backed up at appropriate sites.
- Networks are protected by multiple layers of control including firewalls, Virtual Private Networks (VPN), Intrusion Detection System (IDS) and encryption at the perimeter.
- Databases rely on networks for their protection as well as rigid authentication protocols.
- External electronic transmissions used to receive PII data are encrypted.
- PII data is verified against third-party databases and amended as necessary.
- Significant event recording, review and analysis policies have been implemented.
- The SMCS maintains incident response and disaster recovery plans to minimize the impact of any failures from the previously mentioned measures.

5. **<u>Social Security Numbers</u>. If an SSN is collected and used, describe the purpose of the collection, the type of use and any disclosures.** Also, specify any alternatives that you considered, and why the alternative was not selected.

The SMCS uses the SSN for the following functions:

- To verify identity and determine eligibility to receive a benefit on a loan (such as deferment, forbearance, discharge or forgiveness) under the Federal Family Education Loan Program (FFELP).
- As a unique identifier in connection with the exchange of information between the SMCS and its trading partners (e.g., educational institutions, lending institutions, loan servicers, and consumer reporting agencies) that is performed in association with the servicing of the loans.
- To permit the servicing of the loans.
- As a data component for submission of loan data to the ED NSLDS and Tax Form 1098E data to the Internal Revenue Service (IRS).
- To locate the borrower and to report and collect on the loans in cases of delinquency or default.

The borrower has the option to use the Sallie Mae CIN in place of the SSN during the identification process when communicating and interacting with the SMCS. In the event that the borrower chooses to use the SSN, the SMCS uses the SSN for the following functions:

- To verify borrower identity when establishing an online account with the SMCS. Once the account is created, the borrower receives a UID and a password, which are used for future authentication when using the SMCS borrower online account channels.
- To identify borrowers who call into the customer service call center.

The CIN is not an accepted identifier with trading partners or third-party data platforms that interface with the SMCS.

6. **<u>Uses of the Information</u>**. **What is the intended use of the information?** How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The SMCS will employ the information to support the following capabilities:

- Support for its student loan servicing functions. Operational capabilities include loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, collection, skip-tracing, claims and correspondence history files.
- Provide three major forms of account management and customer access for borrowers. The SMCS currently provides a secure Web site where the borrower can access account information and conduct specific loan transactions. The borrower can also place calls for self service via the IVR or to live customer service agents where the full range of loan services is provided. Finally, the borrower can also mail in forms and other correspondence to the SMCS.
- Transmits specific borrower information data to ED applications such as NSLDS, DMCS and CDDTS.

For data analysis, the SMCS produces error tables during the replication of data and these tables are monitored by internally designed application rules and specific tools (like Dataflux) to ensure the processes are functioning effectively. The systems also perform crosschecks with third-party data sources in order to update internal databases with the latest borrower contact information (addresses, phone numbers and zip codes).

The SMCS uses information from the following commercial, public and Federal databases:

- Consumer reporting agencies in connection with the credit report dispute process.
- Directory Assistance to verify phone numbers.
- NCOA to verify correct addresses for mail-outs.
- NSC and educational institutions for educational data and address verification.
- US postal database to check the validity of zip codes entered and to validate address updates.
- CODE-1 to scrub and standardize postal addresses.
- States' department of motor vehicles for borrower's address verification to support skip-tracing activities.
- Skip trace vendors to verify/obtain updated borrower contact information.
- Tax assessor offices to verify/obtain updated borrower contact information.

7. **Internal Sharing and Disclosure. Which internal ED organizations will the information being shared?** What information is shared? For what purpose is the information shared? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

The SMCS sends data to ED via interfaces to systems such as NSLDS, CDDTS and DMCS. PII data transmitted includes items such as borrower name, maiden name, SSN, driver's license number, date of birth, loan number and loan details.

In accordance with requirements set forth by ED, the SMCS shares the information with ED in order for ED to administer the FFELP program. ED may disclose information contained in a record in an individual's account in accordance with the Privacy Act of 1974.

Risks associated with the internal sharing and distribution of data are covered by the responses to question #4 of this document.

8. **External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)?** What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), MOU or other type of approved sharing agreement with another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The SMCS does not share the information with any external entities, except to process and service the borrower's loans and as permitted by the Privacy Act of 1974. Examples of such external entities include:

Name/Type of Entity	Type of PII Data Shared	Reason for Sharing PII Data
Treasury	SSN and other PII Data	To coordinate the management of borrower payments made through the SMCS or Treasury channels.
Educational institutions	SSN and other PII Data	To coordinate the management of the loan with the educational institution's financial aid office.
Lenders and other loan servicers	SSN and other PII Data	In connection with conversion or de-conversion of loans to/from the SMCS.
Guarantors	SSN and other PII Data	Notification when the loan is put to ED.

Name/Type of Entity	Type of PII Data Shared	Reason for Sharing PII Data
IRS	SSN and other PII Data	In connection with submission of Tax Form 1098E.
Consumer Reporting Agencies	SSN and other PII Data	To report credit history and to resolve credit report disputes.
Skip Trace Vendors	SSN and other PII Data	To obtain updated contact information.
Directory Assistance	Name and contact information	To obtain updated contact information.
States' department of motor vehicles	Driver's license number	To obtain updated contact information.
US Postal Service	Name and contact information	To obtain updated contact information.
NCOA	Name and contact information	To obtain updated contact information.
NSC	Name, contact information and educational institution	To obtain updated contact information and enrollment status.
Employers	Name and contact information	To obtain updated contact information.
References	Name and contact information	To obtain updated contact information.
Operational support vendors	SSN and other PII Data	To provide services to the SMCS in connection with the SMCS' servicing of the ED loans.

The privacy risks arising from external sharing and disclosure fall into the following major categories:

- The ability of authorized/unauthorized employees and unauthorized non-employees to obtain PII during data transmissions to external entities.
- The ability of authorized/unauthorized external entity employees and unauthorized non-employees to access PII from the external entity's database.
- The ability of authorized/unauthorized external entity employees and unauthorized non-employees to alter PII stored in the external entity's database.
- PII data entry errors on the external entity's side.

Key risk mitigation measures for external sharing and disclosure include:

- External electronic transmissions of PII data are encrypted.
- The implementation of significant event recording, review and analysis policies.
- As part of the Customer Information Safeguarding Program, the SMCS establishes data protection protocols with external vendors.
- SMCS' maintenance of incident response and disaster recovery plans to minimize the impact of any failures from the previously mentioned measures.

9. **<u>Notice</u>. Is a notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)?** What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

A privacy notice/policy is presented to the borrower via the following channels:

- Pursuant to the Gramm-Leach-Bliley Act, ED's privacy notice is sent to the borrower by letter or email upon purchase of the loan by ED and on an annual basis thereafter for the life of the loan.

- A privacy policy is also posted on the SMCS' secure borrower Web site, www.ed.manageyourloans.com.
- In order to establish an online account on the SMCS secure borrower Web site, the borrower must agree to the terms of service, which incorporates the privacy policy by reference and link.

The borrower has the opportunity to decline to provide information to the SMCS; however, providing certain information is required in order to (i) communicate with the SMCS through its secure borrower Web site or the SMCS' customer service call center, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness) under the FFELP.

The SMCS does not use the information except to process and service the borrower's ED loans and as permitted by the Privacy Act of 1974.

10**.** **Web Addresses.** List the Web addresses (known or planned that have a Privacy Notice).

- www.ed.manageyourloans.com (borrowers)
- www.opennet.salliemae.com (educational institutions)*

*Note that, while this is a general URL available for all Sallie Mae-interfacing educational institutions, those who meet requirements and are granted access to view servicing information retrieved from the ED database associated with borrowers from their school will be able to view ED variations of the OpenNet Web pages. These Web pages carry the following privacy policy link: http://www.salliemae.com/about/privacy_ed.htm.

11. **Security. What administrative, technical and physical security safeguards are in place to protect the PII?** Examples include monitoring, auditing, authentication, firewalls, etc. Has a Certification and Accreditation (C&A) been completed? Is the system compliant with any federal security requirements? If so, which federal security requirements?

The SMCS system has implemented the following groups of technical and operational controls:

- System and information access security utilizes a variety of network-based measures including, but not limited to, centralized active directory management, firewalls, secure connections, encryption, remote access VPNs and password policy enforcement (including strength, rotation, etc.). These are complemented by user identification and authentication procedures that involve cross-verification of select PII with internal databases.
- Other operating policies include regular security and patch updates, a centrally monitored configuration management plan, database backup and operations redundancy/failover guidelines, disposal of key operating assets as well as physical and environmental protection.
- All SMCS personnel are required to obtain government security clearance and complete ED's initial Security Training and Awareness course as well as periodic refresher training.
- The SMCS also maintains a Contingency Plan and Incident Response Plan covering equipment, personnel and procedures.

Please refer to the responses in question #4 for other administrative, technical and physical security safeguards.

These controls are buffered by security policies that include significant event recording and audit, periodic Risk Assessments and Certification and Accreditation, as well as System and Services Acquisition oversight by the FISMA Program Management Office.

The SMCS is currently undergoing a Certification and Accreditation exercise for the ED Title IV loan management servicing contract.

The SMCS' controls are compliant with the applicable FISMA and NIST standards. These include FIPS 199 for security categorization, NIST SP 800-53 Rev 2 and 800-30 for control selection and augmentation. The SMCS Certification and Accreditation documentation policies comply with NIST SP 800-37 and NIST SP 800-18. As part of regular operations, the SMCS utilizes checklists and procedures derived from NIST 800-70 and 800-37.

12. **Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a?** Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

Intentionally left blank, to be completed by the ED Privacy Officer.

13. **Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected?**

The SMCS will be utilizing the ED records retention and disposition schedule.

Certifying Officials Signatures:

Jonathan E. Kroehler, **System Owner**	9-11-09 **Date**
Gregory Plenty, **Program Office Computer Security Officer**	**Date**

For systems that collect, maintain and or transfer SSNs:

William Leith, **Senior Program Official**	**Date**