Privacy Impact Assessment (PIA) for the
Private Collection Agencies (PCAs)

This PIA was approved on May 3, 2018 and reviewed on Jan 24, 2018 by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Calvin Whitaker
Contact Email: Calvin.Whitaker@ed.gov

System Owner

Name/Title: Diana O'Hara
Program Office: Federal Student Aid (FSA)

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.
Please complete this Privacy Impact Assessment (PIA) on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. If a question does not apply to your system, please answer with N/A.

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

This Privacy Impact Assessment (PIA) covers the following Private Collection Agencies (PCAs) and the respective systems they operate on behalf of Federal Student Aid (FSA) to support the Student Aid Fiscal Responsibility Act (SAFRA), and the Debt Collection Improvement Act (DCIA) Not-For-Profit Loan Servicing Processing operations. PCA's systems perform the following functions: borrower account management, interim/repayment servicing, borrower correspondence, call scheduling, collection, skip-tracing, and correspondence history files. PCA systems communicate with internal FSA platforms, borrowers, other loan servicers, third-party providers, consumer reporting agencies, and government agencies (as permitted by the Privacy Act of 1974). Channels of communication include U.S. mail, telephone calls, a secure borrower website, secure email, and secure data transfer links. See Appendix A for complete list of active PCAs.

1.2 N/A Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained or shared.

The information is collected, stored, and updated by PCAs on behalf of the Department of Education Office of Federal Student Aid, is used to enable the effective location and recovery of defaulted student loans. The information is used only to support the collection or administrative resolution of the debts associated with a borrower's defaulted student loan(s) and to provide additional processing capacity and augment the U.S. Department of Education, Office of Federal Student Aid Debt Management and Collection System (DMCS) Major Application.

1 The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf](https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf)
1.3 □ N/A Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 □ N/A Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

Updated PIA

Original Publication Date: 02/10/2015

1.5 □ N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

*If you are unsure of your legal authority, please contact your program attorney.*

2.1 □ N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?


2.2 □ N/A Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer YES or NO.

Yes
2.2.1 □ N/A If the above answer is YES this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s)). Please provide the SORN name and number, or indicate that a SORN is in progress.

PCAs are covered under the following System of Records Notice: "Common Services for Borrowers (CSB) Contract, "SORN #18-11-16 Federal Register 3503-3507. Federal Register date September 2, 2016.

Records Management

*If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov.*

2.3 □ N/A Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

DOED Record Schedule: 075
Title: FSA Loan Servicing, Consolidation, and Collection Records
NARA Disposition Authority: N1-441-09-16
Disposition Instructions:

*Record copy (temporary)- cut off annually upon payment or discharge of loan. Destroy/delete 15 years after cut off.*

---

2 A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. [https://connected.ed.gov/om/Documents/SORN-Process.pdf](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4 N/A Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer YES or NO.

Yes

3. Characterization and Use of Information

Collection

3.1 N/A List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

PCAs collect and maintain the following PII data pertaining to borrower/co-borrower/co-signers/students:

- Full Name
- Maiden Name
- Social Security Number
- Bank Account Numbers
- Student Loan Account Number
- Alien Registration Number
- Date of Birth
- Home Address
- Related Demographic Data
- Home, Work, Alternate. Mobile Telephone Numbers
- Financial Information
- Checking Account Information
- Email Address
- Employment Information

3.2 N/A Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer YES or NO.

Yes

3.3 N/A What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.)?

The sources of information are Federal Student Aid's Debt Management Collection System (DMCS) and obtained from schools/educational institutions, lenders/financial institutions, employers, US Department of Education (DoED), National Student Clearing house (NSC), external database directory assistance, consumer reporting agencies, skip-tracing vendors, U.S. Military, commercial person locater services, and U.S. Department of Treasury.
3.4 N/A How is the information collected from stated sources (paper form, web page, database, etc.)?

The information is collected via the following channels:
- Phone calls with customer service agent
- Entries via the Interactive Voice Response (IVR) service
- Incoming correspondence (e.g., via U.S. mail, email, etc)
- Entry via the Borrower Portal Website (https://myeddebt.ed.gov)
- Bulk file transfer from third-party data providers
- As required, secure data transmission from DoED applications, such as: Debt Management Collection System (DMCS).

3.5 N/A How is this information validated or confirmed?³

The information is validated via identity verification and authentication during online account creation and telephone calls, verification between internal databases within systems, and data exchange with external trading partner databases such as:
- Consumer reporting agencies
- Other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system

³ Examples include form filling, account verification, etc.
Use

3.6 N/A  Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The use of data collected enables the effective location, recovery and/or administrative resolution of defaulted student loans on behalf of and under contract with the U.S. Department of Education, Office of Federal Student Aid. This information is vital to ensure every effort has been made to contact borrowers to allow them every opportunity to resolve their debt and get their student loans back in good standing with the Department of Education.

3.7 NO  Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

3.7.1 N/A  If the above answer is YES, what controls are in place to minimize the risk and protect the data?
3.8 □ N/A Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

| No |

3.8.1 □ N/A If the above answer is YES, please explain.

Social Security Numbers

*It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

3.9 □ N/A Does the system collect Social Security Numbers? Please answer YES or NO.

| Yes |

3.9.1 □ N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

The SSN is the unique identifier for Title IV student financial assistance programs and it's required by program participants and their trading partners to satisfy borrower identification, borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. Trading partners include the Department of Education, Internal Revenue Service, Department of Homeland Security, Selective Service System, institutions of higher education, national credit bureaus, skip-trace vendors, employers, lenders and servicers. To the extent possible, PCAs inform the user of other unique identifiers in lieu of the SSN, such as account numbers, but the SSN is the required identifier for numerous business processes.
3.10 N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

4. Notice

4.1 N/A How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

A privacy notice is presented to the borrower via the following channels:
Free Application for Federal Student Aid (FAFSA) form and on the FAFSA on line application website (www.fafsa.ed.gov).
In order to establish an on-line account with a specific PCA, the borrower must agree to the Term of Service, which incorporates the privacy policy by reference and link.
PCAs will send a written Privacy Notice to borrowers when they initially convert to the PCA system and annually thereafter.
4.2 N/A  Provide the text of the notice, or the link to the webpage where the notice is posted.

See Appendix C.

4.3 N/A  What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The borrower has the opportunity to decline to provide the information to a PCA; however providing certain information is required in order to (i) communicate with the PCA system through its secure borrower portal website or customer service call center, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness). PCAs use the information only to process and service the borrower’s DoED loans and as permitted by the Privacy Act of 1974.

5. Information Sharing

Internal

5.1 N/A  Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
The information collected and processed by PCAs is shared with the U.S. Department of Education.

The sharing of information with Federal Government agencies is pursuant to a Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) and/or other contractual or regulatory requirements. Sharing of information with certain other entities (consumer reporting agencies, independent program participants, etc.) will be pursuant to contractual or regulatory requirements or through sharing agreements between the applicable entities and the Department of Education.

External

Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)? Please answer YES or NO. If the answer is NO, please skip to Question 5.8.

Yes
PCAs share information data with the following external entities:

- National Credit Bureaus
- Letter Service
- Postal Service
- Collection Software Systems
- Skip-Tracing Vendors (Lexis Nexus, Accurint, CBC Innovis, Trans Union LLC, Experian, Equifax)
- Educational Institutions (to coordinate the management of the loan with the educational institution's financial office)
- Direct Loan Servicers, and other servicers
- Independent Auditors
- National Consumer Reporting Agencies (to obtain updated contact information and enrollment status)
- Person locator services (to obtain updated contact information)
- Other parties as authorized by the borrower (employers, references)
- National Change of Address (to obtain updated mailing address information)
- Optional support vendors
- Contractors Fulfillment Vendors, Universal Mail Delivery Service, Sound-Bite Communications

The information is only shared as required to complete the Federal Student Aid business related to the student loans. Information shared outside of the Department of Education is shared through secure encrypted transmission and email.
5.7 □ N/A How is the information shared and used by the external entity?

PCAs only 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. The information is only shared as required to complete the Federal Student Aid business related to the student loans. Information shared outside of the Department of Education is shared through secure encrypted transmission and email.

External users (e.g., contractors, school financial aid officers) access our systems and data using a user name and password, and/or a PIV card and PIN number. External partners use a secure data transmission of machine-to-machine transfer with external entities such as skip-tracing vendors.

5.8 □ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

Yes

5.9 □ N/A Does the project place limitation on re-disclosure? Please answer YES or NO.

Yes

6. Redress

6.1 □ N/A What are the procedures that allow individuals to access their own information?

Procedures for allowing individuals to access their own information are explained in the System of Records notice listed in question 2.2. In addition, borrowers may access their own information via link. (https://studentaid.ed.gov/sa/repay-loans/default and https://myeddebt.ed.gov.

---

4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.
6.2 N/A What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Procedures for allowing individuals to correct inaccurate or erroneous information are explained in the System of Records notice listed in question 2.2.

6.3 N/A How does the project notify individuals about the procedures for correcting their information?

The System of Records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1 N/A Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer YES or NO.

Yes
7.2 N/A What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

Access to FSA information is governed by the concepts of least privilege and separation of duties. All system access is granted by predefined roles and privileges, and all FSA system users must undergo a Federal background security clearance process.

7.3 N/A What administrative, technical, and physical safeguards are in place to protect the information?

In accordance with the Federal Information Security Management Act of 2002 (FISMA), every PCA must receive a signed Authority To Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program. FISMA controls implemented by each PCA comprise a combination of management, operational and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environment protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management. The Department will follow all Federal laws, standards and guidelines and Department of Education policies each PCAs must comply with.

7.4 N/A Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

7.5 N/A Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 □ N/A Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 □ N/A Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 □ N/A Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

Quarterly authenticated network and operating vulnerability scans and network penetration testing is conducted to ensure the security of PCAs network environment. Security audits are performed on an annual basis by authorized third parties to ensure the controls in place are effectively securing our data. PCAs are required to submit PO&AMs to FSA quarterly which continuously monitor any vulnerabilities and ensure that they are mitigated and closed.

8. Auditing and Accountability

8.1 □ N/A How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

The system owner ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed and identifying applicable Privacy Act SORNs, by ensuring Privacy Act records are maintained in accordance with the provisions of the Privacy Act and the published SORN, by ensuring appropriate security and privacy controls are implemented to restrict access, and properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA’s Life-cycle Management Methodology, which addresses security and privacy risks throughout the system’s life-cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of Records notices, memorandum of understanding, etc.
Privacy risks associated with PCAs include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by granting access to only authorized individuals based on their respective position and need to know basis, limiting users who are screened and utilizing least privilege principles, masking account number, routing number, and check digit number when viewed, and encrypting data in transmission. Updating security patches per the patch scheduling and updating devices’ operating software, amongst other software.
APPENDIX C

The Privacy Act of 1974 (5 U.S.C. 552a) requires that the following notice be provided to you:

The authority for collecting the requested information from and about you is 421 et seq. of the Higher Education Act of 1965, as amended (20 U.S.C. 1071 et seq). The principal purpose for collecting the information about you on this website is to allow the electronic servicing of your loan. Your disclosure of the requested information is voluntary, but you must provide the requested information in order to participate in electronic servicing of your loan. The information in your file may be disclosed, on a case-by-case basis or under a computer matching program, to third parties as authorized under routine uses in the appropriate systems of records notices. The routine uses of this information includes, but not limited to, its disclosure to federal, state, or local agencies, to private parties such as relatives, present and former employers, business and personal associates, to consumer reporting agencies, to financial and educational institutions and to guaranty agencies in order to verify your identity, to determine your eligibility to receive a loan or a benefit on a loan, to permit the servicing or collection of your loan(s), to enforce the terms of the loan(s), to investigate possible fraud and to verify compliance with federal student financial aid program regulations or to locate you if you become delinquent in your loan payments or if you default. To provide default rate calculations, disclosures may be made to guaranty agencies, to financial and educational institutions, or to state agencies. To provide financial aid history information, disclosures may be made to educational institutions. To assist program administrators with tracking refunds and cancellations, disclosures may be made to guaranty agencies, to financial and educational institutions, or to federal or state agencies. To provide a standardized method for educational institutions to effectively submit student enrollment status, disclosures may be made to guaranty agencies or to financial and educational institutions. To counsel you in repayment efforts, disclosures may be made to guaranty agencies, to financial and educational institutions, or to federal, state, or local agencies.

In the event of litigation, we may send records to the Department of Justice, a court, adjudicative body, counsel party, or witness if the disclosure is relevant and necessary to the litigation. If this information, either alone or with other information, indicates a potential violation of law, we may send it to appropriate authority of action. We may send information to members of Congress if you ask them to help you with federal student aid questions. In circumstances involving employment complaints, grievances, or disciplinary action, we may disclose relevant records to adjudicate or investigate the issues. If provided for by a collective bargaining agreement, we may disclose records to labor organization recognized under 5 U.S.C. Chapter 71. Disclosures may be made to our contractors for the purpose of performing any programmatic function that requires disclosure of records. Before making any such disclosure, we will require the contractor to maintain Privacy Act safeguards. Disclosures may also be made to qualified researchers under Privacy Act safeguards.

The effective date of our Online Consumer Information Privacy Policy is April 15, 2011. It replaces all prior online information privacy policies issued by PCA’s with respect to this website. We reserve the right to change our Online Consumer Information Privacy Policy.”