Privacy Impact Assessment (PIA)

for the

Private Collection Agencies (PCA's)

1/27/2020

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Scot Ceravolo
Contact Email: scot.ceravolo@ed.gov

System Owner

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

Please submit completed Privacy Impact Assessments to the Privacy Office 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.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

This Privacy Impact Assessment (PIA)) covers all Private Collection Agencies (PCAs) systems and the respective systems they operate on behalf of Federal Student Aid (FSA) to support the Student Aid Fiscal Responsibility Act of 2009 (SAFRA), and the Debt Collection Improvement Act of 1996 (DCIA), Not-For-Profit Loan Servicing Processing operations. PCA systems perform the following functions: borrower account management, interim/repayment servicing, borrower correspondence, call scheduling, collection, skip-tracing, and other correspondence history files. PCAs communicate with internal FSA platforms, borrowers, other loan servicers, third-party providers, consumer reporting agencies, and government agencies.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

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

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

[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. OMB Circular A-130, page 33

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

Yes

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Higher Education Act of 1965 (Public Law 89-329), as amended, section 428,484, and 485B:31 U.S.C 7701: and Executive Order 9379 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

PCA's are covered 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.

[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://www.federalregister.gov/documents/2016/09/02/2016-21218/privacy-act-of-1974-system-of-records

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

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. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

DOED Record Schedule: 075
Title: FSA Loan Servicing, Consolidation, and Collection Records
NARA Disposition Authority: N1-441-09-16
Disposition Instruction: Record copy (temporary)- cut off annually upon payment or discharge of loan. Destroy/delete 15 years after cut off.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

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

- Full Name
- Maiden Name

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

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

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

The source of information is from FSA's Debt Management and Collection System (DMCS) and obtained from schools/education institutions, lenders/financial institutions, employers, U.S. Department of Education (DoED), National Student Clearing House (NSC), external database directory assistance, consumer reporting agencies, skip-tracing vendors, U.S. Military, commercial person locator, and U.S, Department of Treasury.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Information is retrieved via the following channels:

- Phone calls with customer service agents
- Entries via Interactive Voice Response (IVR) service
- Incoming correspondence
- 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 Collections System (DMCS).

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The information is validated via identity verification and authentication during on-line account creation and telephone calls, verification between internal database systems, and data exchange with external trading partner database such as: Consumer Reporting agencies, other loan servicers, Directory Assistance, and National Change of Address (NCOA) system.

Use

3.6. Describe how the PII is used 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 resolve their debt and get their student loans back in good standing with the DoED.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

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] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

The SSN is the unique identifier for Title IV student financial assistance program, and it's required by program participants and their trading partners to satisfy identification, borrower identification, borrower eligibility, loan servicing, and loan status reporting requirements under law and regulation. Trading partners include the Depart 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.

3.8.2. Specify any alternatives considered in the collection of SNNs and why the alternatives were not selected.

☐ N/A

There are no alternatives to consider for the collection of the SSN, SSN is a unique identifier required by program participants and their trading partners, to the extent possible, PCA's 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.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? 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 (https://studentaid.gov/h/apply-for-aid/fafsa).
In order to establish an on-line account with a specific PCA, the borrower must agree to the Terms of Service, which incorporates the privacy policy by reference and link.
PCA's will send a written Privacy Notice to borrowers when they initially covert to the PCA system and annually thereafter.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

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 mad e to guaranty agencies, to financial and educational institutions, or to federal, state, or local agencies. In the event of ligation, 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 ligation. 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"

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The borrower has the opportunity to decline the provided information to the 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) receiver certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness. PCA's use the information only to process and service the borrowers DoED loans as permitted by the Privacy Act of 1974.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

☑ N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

Click here to enter text.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

PCA's share information data with the following external entities:

- Nation Credit Bureaus
- Letter services
- Postal services
- Collection software systems
- Skip-tracing vendors (Lexis Nexus, Accurint, CBS Innovis, Trans Union, LLC, Experian, Equifax)
- Education institutions (to coordinate the management of the loan with the educational institution's financial office)
- Direct Loan Services, 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, and Sound Bites Communication.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

The information is only shared as required to complete the FSA business related to the student loans. Information shared outside of the DoED is shared through secure encrypted transmission and email.

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

PCA's only share information with an external entity to process the borrower's loans as permitted by the Privacy Act of 1974. The information is only shared as required to complete the FSA business related to the student loans. Information shared outside of the DoED is shared through secure encrypted transmission and email.

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

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

Yes

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

6.1. 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 (SORN) listed in question 2.2.1 In addition, borrowers may

access their own via link. (https://studentaid.gov/manage-loans/default and https://myeddebt.ed.gov/.

6.2. 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 (SORN) listed in question 2.2.1

6.3. How does the project notify individuals about the procedures for correcting their information?

System of Records Notice (SORN) listed in question 2.2 explains the procedure for correcting customer information.

7. Safeguards

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

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. 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 of a combination of management, operation, 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 environmental protection, planning, personnel security, risk assessment, system and service acquisition, system and communication protection, system and information integrity, and program management. The Department and PCA's will follow all Federal laws, standards, and guidelines and DoED policies.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

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

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII 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 risk are properly assessed and identify applicable Privacy Act SORN's, 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 life-cycle Management methodology, which addresses security and privacy risk throughout the systems life cycle.

Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of Records Notice, memorandum of Understanding, etc.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risk associated with PCA's 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 cost.
The risks are remediated 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 privileges, masking account number, routing number, and digital check number when viewed, and encryption data in transmission. Updating security patches per patch scheduling and updating devices operating systems, amongst other software.