



Privacy Impact Assessment

For:

Private Collection Agencies (PCAs)
(See Section 1 for a listing of each individual PCA)

Date:

September 2012

Point of Contact:

Theon S. Dam
202-377-3106
Theon.S.Dam@ed.gov

System Owner:

Keith Wilson
202-377-3591
Keith.Wilson@ed.gov

Author:

Mike K. Murray
Mike.Murray@ed.gov
202-377-3128

**Federal Student Aid
U.S. Department of Education**



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

This privacy impact assessment covers the following private collection agencies (PCAs) and the respective systems they operate on behalf of Federal Student Aid (FSA) to support FSA Student Aid and Fiscal Responsibility Act (SAFRA) Not-For-Profit Loan Servicing Processing operations.

PCA Name	Information System Name and Website URL
Account Control Technology (ACT)	Account Control Technology Loan Data System www.accountcontrol.com
Allied Interstate - iQOR	iQOR Intellione System www.iqor.com
The CBE Group, Inc.	The CBE Group, Inc. Collection System www.cbegroup.com
Coast Professional	Coast Account Receivables Database www.coastprofessional.com
Collection Technology, Inc. (CTi)	CTi Collection System www.collectiontechnology.com
Collecto, Inc. (CCA)	Flexible Automated Collection System www.eos-cca.com
ConServe	ConServe Collection Management System www.conserve-arm.com
Diversified Collection Services (DCS)	Diversified Collection Services Collection System www.performantcorp.com
Delta Management Associates (DMA)	Delta Management Associates Debt Collection System www.deltamanagementassociates.com
Enterprise Recovery Systems, Inc. (ERS)	Enterprise Recovery Systems Safenet www.ersinc.com
Financial Asset Management Systems, Inc. (FAMS)	BFrame Collection System www.fams.net
Financial Management System (FMS)	FMS Inteltec Collection System www.fmsdc.com
Gatestone (formerly Collectcorp)	Gatestone Receivables Management System www.gatestoneco.com
GC Services, LLC	Student Loan Collection System www.gcserv.com
Immediate Credit Recovery (ICR)	BFrame Recovery Management System www.icrcollect.com
NCO Financial Systems, Inc.	Flexible Automated Collection System www.ncogroup.com
National Recoveries, Inc. (NRI)	NRI Inteltec Collection System www.nationalrecoveries.com
Pioneer Credit	Collection Resource System www.salliema.com
Premiere Credit of North America	Flexible Automated Collection System www.premierecredit.com



Progressive Financials Services, Inc.	Progressive Financial Services Collection System www.progressivefinancial.com
Van Ru Credit Corporation	Van Ru Credit Corporation Collection System www.vanru.com
West Asset Management (WAM)	Flexible Automated Collection System www.west.com
Windham Professional, Inc. (WPI)	eCollections Platform www.windhampros.com

PCA systems perform the following functions: borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, borrower correspondence, call scheduling, collection, skip-tracing, and correspondence history files.

PCA systems communicate with internal FSA platforms, borrowers, other loan servicers, third-party data providers, consumer reporting agencies, guarantors 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.

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 Higher Education Act of 1965 (HEA), As Amended, Section 441 and 461 Title IV, Section 401.

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

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

- Full name
- Maiden name
- Social Security Number (SSN)
- Bank account numbers
- Student Loan account number
- Driver's license number and state
- Alien registration number
- Date of birth
- Home address
- Related demographic data
- Home, work, alternate, mobile telephone number



- Financial Information
- Checking account information
- Email address
- Employment information
- Medical information (to the extent required for purposes of certain deferments and discharge requests) and
- Borrower loan information including: disbursement amount, principal balance, accrued interest, loan status, repayment plan, repayment amount, forbearance status, deferment status, separation date, grace period, and delinquency status.

The information is obtained from the student/borrower, co-borrowers, co-signers, references provided by the borrower, educational institutions, financial institutions, employers, U.S. Department of Education (DoED), the National Student Loan Data System (NSLDS), National Student Clearinghouse (NSC), external database (e.g., Directory Assistance, consumer reporting agencies, and skip-trace vendors, U.S. Military, commercial person locator services, and U.S. Department of the Treasury).

The information 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 Borrower Portal Web site (<https://EdManage.MyEdLoan.com>)
- Bulk file transfer from third-party data providers
- As required, secure data transmission from DoED applications, such as: NSLDS and Debt Management Collection System (DMCS), etc. and
- Secure data transmission from the U.S. Department of the Treasury.

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

- Consumer reporting agencies
- Other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system and
- 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 any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.**



The 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 chance to resolve their debt and get their student loans back in good standing with the Department of Education.

Privacy risks are mitigated through multiple security and program reviews, the implementation of required Federal security and privacy controls, and a continuous monitoring program (see section 11 for more detail).

Other controls to minimize privacy risks include the following:

- Extensive collection training is provided at the time of hire and a minimum of annually thereafter to ensure no Personally Identifiable Information is released to unauthorized third parties
- Encryption is utilized in all transmission of sensitive data
- Network security controls are in place to prevent unauthorized access to any sensitive data, including firewall technology, intrusion detection systems, file integrity monitoring, antivirus and malware protection
- Security audits are performed on an annual basis by authorized third parties to ensure the controls in place are effectively securing our data
- Regular vulnerability scans and network penetration tests are performed to ensure the security of our network environment

5. Social Security Number (SSN). 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. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The SSN is the unique identifier for Title IV student financial assistance programs and its use is 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, lenders, and servicers.

To the extent possible, PCAs employ the use of other unique identifiers in lieu of the SSN, such as account numbers, but the SSN is the required identifier for numerous business processes.

6. Uses of the Information. 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 information collected, stored, and updated by PCAs on behalf of the U.S. Department of Education, Office of Federal Student Aid, is used to enable the effective location, recovery and/or administrative resolution 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's Debt Management and Collections System (DMCS) Major Application.

7. Internal Sharing and Disclosure. With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

Information collected and processed by PCAs is shared with the following internal organizations:

Federal Agencies

- U.S. Department of Education, Office of Federal Student Aid
- Contractors and Vendors
- Fulfillment vendors
- Universal Mail Delivery Service
- Soundbite Communications
- Immedia

Skip Tracing vendors

- LexisNexus
- Accurint
- CBC Innovis
- Trans Union LLC
- Experian
- Equifax

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), Memorandum of Understanding or other type of approved sharing agreement with another agency?

PCAs share data with the following external entities:

- National Credit Bureaus
- Letter service
- Skip-tracing service
- Postal Service
- Collection Software Systems
- Other Skip Tracing Vendors



- Educational institutions (to coordinate the management of the loan with the educational institution's financial aid 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) and
- Optional support vendors.

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

Sharing of information with Federal government agencies will be 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.

See response to Section 4 hereof to review the risk to privacy from external sharing and disclosure and how the risks are mitigated.

9. Notice. Is 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:

- A privacy notice is provided on the Free Application for Federal Student Aid (FAFSA) form and on the FAFSA online application website (www.fafsa.ed.gov)
- In order to establish an online account with a specific PCA, 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 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.



PCAs will send a written Privacy Notice to borrowers when they initially convert to the PCA system and annually thereafter. The following will be posted on the PCA's website:

“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 include, but are 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 efficiently 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 the appropriate authority for 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 actions, we may disclose relevant records to adjudicate or investigate the issues. If provided for by a collective bargaining agreement, we may disclose records to a 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 this Online Consumer Information Privacy Policy is April 15, 2011. It replaces all prior online information privacy policies issued by PCA with respect to this website. We reserve the right to change our Online Consumer Information Privacy Policy.”

Any changes to our Online Consumer Information Privacy Policy will be reflected in the updated version displayed at our corresponding websites.

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



Each PCA website has its own Privacy Notice (See Section 1 for list of web addresses that contain PCA-specific Privacy Notices). There is also a Privacy Notice located at the following website: www.fafsa.ed.gov

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 C&A been completed? Is the system compliant with any federal security requirements?

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. For specific dates on which individual PCAs received their ATOs, contact the point of contact listed on the title page of this document.

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 environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

PCAs comply with the following Federal laws, standards, and guidelines:

- Federal Information Security Management Act of 2002
- Privacy Act of 1974
- E-Government Act of 2002
- Federal Information Processing Standards Publications (FIPS PUBS) on IT Security
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010
- NIST SP 800-35, Guide to Information Technology Security Services, October 2003
- NIST SP 800-37, Rev. 3, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
- NIST SP 800-40, Procedures for Handling Security Patches, November 2005
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, September 2009
- NIST SP 800-42, Guidelines on Network Security Testing, October 2003
- NIST SP 800-44, Rev. 2, Guidelines on Security Public Web Servers, September 2007
- NIST SP 800-45, Rev. 2, Guidelines on Electronic Mail Security, February 2007
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002



- NIST SP 800-50, Building an Information Technology Security Awareness Program, October 2003
- NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems, August 2009
- NIST SP 800-55, Rev. 1, Performance Measurements Guide for Information Security, July 2008
- NIST SP 800-58, Security Considerations for Voice Over IP Systems, January 2005
- NIST SP 800-60, Rev. 1, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-60, Rev. 1, Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
- NIST SP 800-61, Rev. 1, Computer Security Incident Handling Guide, March 2008
- NIST SP 800-64 Rev. 2, Security Considerations in the Systems Development Life Cycle, October 2008
- NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process. January 2005
- NIST SP 800-70, Rev. 2, National Checklist Program for IT Products: Guidelines for Checklists Users and Developers, February 2011
- NIST SP 800-77, Guide to IPsec VPNs, December 2005
- NIST SP 800-81, Rev. 1, Secure Domain Name System (DNS) Deployment Guide, April 2010
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005
- NIST SP 800-88, Guidelines for Media Sanitization, September 2006
- NIST SP 800-92, Guide to Computer Security Log Management, September 2006
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- NIST SP 800-95, Guide to Secure Web Services, August 2007
- NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
- NIST SP 800-113, Guide to SSL VPNs, July 2008
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, April 2010
- NIST SP 800-123, Guide to General Server Security, July 2008 and
- NIST SP 800-124, Guidelines on Cell Phone and PDA Security, October 2008



Department of Education Policies:

- Department of Education Handbook for Information Technology Security
- Department of Education Handbook for Information Technology Security General Support
- System and Major Application Inventory Procedures
- Department of Education Handbook for Certification and Accreditation Procedures
- Department of Education Handbook for Information Technology Security Configuration Management Procedures
- Department of Education Handbook for Information Technology Security Contingency Planning Procedures
- Department of Education Information Technology Security Test and Evaluation Plan Guide
- Department of Education Incident Handling Program Overview
- Department of Education Handbook for Information Technology Security Incident Handling Procedures
- Department of Education Information Technology Security Training and Awareness Program Plan.

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?

PCAs are covered under the following System of Records Notice: “Common Services for Borrowers (CSB) Contract,” SORN # 18-11-16, 71 *Federal Register* 3503-3507.

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? If yes – provide records schedule number:

Per FSA, PCAs manage records in accordance with the following records schedule: “FSA Loan Servicing, Consolidation, and Collections Records.” The ACS Tracking Number is OM: 6-106:L74.

DoED Record Schedule:

Schedule Locator NO: 075

Draft Date: 03/11/2009

Title: FSA Loan Servicing, Consolidation, and Collections Records

Principal Office: Federal Student Aid

NARA Disposition Authority: N1-441-09-16

Description:

These records document business operations that support the servicing, consolidation, and collection of Title IV federal student aid obligations. These records relate to the post-



enrollment period of student aid, including servicing of direct loans, consolidation of direct loans, managing and recovering defaulted debts assigned to the Department from Federal Family Education Loan (FFEL) and other lenders, rehabilitated loans, and any other type of Title IV student aid obligation.

This schedule provides a common disposition for records that comprise a variety of material and media, including but not limited to demographic and financial data on individual borrowers; institutional data on schools, guarantors, lenders, private collection agencies; records of financial transactions, payments, collections, account balancing and reconciliation, and reporting; records pertaining to customer interactions; and related correspondence and documents.

As these records may be maintained in different media formats, this schedule is written to authorize the disposition of the records in any media (media neutral). Records that are designated for permanent retention and are created and maintained electronically will be transferred to NARA in an approved electronic format.

DISPOSITION INSTRUCTIONS:

- a. Record Copy
TEMPORARY
 - Cut off annually upon payment or discharge of loan. Destroy/delete 15 years after cut off.
- b. Duplicate Copies Regardless of Medium Maintained for Reference Purposes and That Do Not Serve as the Record Copy
TEMPORARY
 - Destroy/delete when no longer needed for reference.

ELECTRONIC INFORMATION SYSTEMS:

Direct Loan Servicing System (DLSS)
Direct Loan Consolidation System (DLCS)
Conditional Disability Discharge Tracking System (CDDTS)
Debt Management and Collection System (DMCS)
Credit Management Data Mart (CMDM)

IMPLEMENTATION GUIDANCE:

Follow the disposition instructions in DoED 086 for system software; input/source records; output and reports; and system documentation. Original signed paper documents required for legal purposes must be kept for the full length of the retention period, even if an electronic version has been captured in the information system.

ARRANGEMENT / ANNUAL ACCUMULATION:

PREVIOUS DISPOSITION AUTHORITY:



SPECIFIC LEGAL REQUIREMENTS:

Title IV of the Higher Education Act (HEA) of 1965, as amended

SPECIFIC RESTRICTIONS:

Privacy Act 18-11-05 Title IV Program Files

Privacy Act 18-11-08 Student Account Manager System

BUSINESS LINE: Loans