



**Privacy Impact Assessment
For the US Department of Education
From**

Enterprise Recovery Systems, Inc.

Date

March 20, 2009

Contact Point

System Owner: Jeff Bassett

Author: Jeff Bassett (Chief Information Officer)

1. What information will be collected for the system?

Information regarding debts placed for collection from The US Department of Education.

Full Name

Address

SSN

Phone

E-mail

Employment Information to include current and past employment not to exceed 5 years

Debtor Information to include:

Disbursement amount, principal balance

Interest accrual, loan status

Repayment plan

Repayment amount

Separation date

Default s

2. Why is this information being collected?

- (1) Enterprise Recovery Systems, Inc. (ERS) is a collection agency contracted by The US Department Education to collect on federally funded student loans. The information collected will only be used to collect defaulted accounts as defined by the contract award.
- (2) Official correspondence to debtors from US Dept of Education and ERS.

3. How will FSA use this information?

ERS will provide information updates to the US Department of Educations system

ERS will use applicable information to collect outstanding/collection accounts for the US Dept of Education

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

ERS will release information as required in collection of debts from outstanding parties and will seek outside assistance to perform this to determine debtor location, financial capabilities, work histories, and current credit reporting agency information as determined by the following organizations:

CDW Berbee
Credit Bureaus (Trans Union, Experian)
CR Software
IBM
Lexis Nexis
Livevox
PSC Info Group
Recall
First Data
CBC Innovis
Teletrek
Talx

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

The Mini Miranda is included in all ERS correspondence sent to debtors. All companies that work with ERS are required to sign off on the following Confidentiality Agreement.



Date

COMPANY NAME
Attn: Authorized Person
Street address
City, State Zip

Dear Mr. or Ms. Authorized Person:

The Gramm Leach Bliley Act of 2002 requires Enterprise Recovery Systems, Inc., as a Collection Agency in compliance under the Act, to implement plans to safeguard the disclosure of non-public personal information. This federal law mandates that ERS, Inc. must take reasonable steps to select and retain service providers who maintain appropriate security safeguards for covered data information.

The information provided to COMPANY NAME by Enterprise Recovery Systems, Inc. is protected from disclosure by the Privacy Act of 1974, as amended. The Protection of this information, once entrusted to COMPANY NAME, becomes your responsibility. Therefore, COMPANY NAME agrees to protect the privacy of all information that has been provided to you. COMPANY NAME does understand that the criminal penalties may be enforced if COMPANY NAME should violate the requirements of the Privacy Act.

The purpose of this letter is to document assurance of your compliance with these requirements, including but not limited to implementing a policy regarding the safeguard of customer information and the requisite training of your employees.

A signature below by an authorized representative of your company shall signify that COMPANY NAME shall keep confidential any and all non-public personal information provided by or obtained on behalf of ERS, Inc. regarding a customer. Only authorized employees of COMPANY NAME who need to see non-public personal information about a consumer in order to fulfill their employment function shall have access to such information.

ERS, Inc. values its business relationship with COMPANY NAME. If you do not concur with our understanding of these federal requirements or if you have any questions, please contact me at your earliest convenience. Your prompt response within the next 10 business days is greatly appreciated.

Sincerely,

Jeff Bassett
Sr. Vice President

Signed by Authorized Representative of Company Name

Printed Name

Date

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

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

The Enterprise Recovery Systems, Inc. will not further disclose the information except as defined by the System of Records Notice in the interest of the U.S. Government and the Department of Education. Enterprise Recovery Systems, Inc. company privacy policy also restricts the sharing of information.

6. How will the information be secured?

ERS has identified and secured the systems housing debtor information (as defined in question one of this document), with the following design and policy in place:

ERS production debtor systems are segmented from the Local Area Network and Wide Area Network by Firewalls, Intrusion Detection systems and virtual Local area Network segments (VLAN's).

Access Control to these systems are controlled by multiple sign-off at a senior level of the organization and reviewed quarterly, access is based on 'least privilege' and is role based. Policies are in place for termination of employees and change of role to ensure that access rules change with status. Monitoring and audit logs are in place to ensure tracking of access. Password policies follow industry best practices to ensure complexity, change schedule and lockout in the event of failed attempts. There is segregation of duties between those who authorize access to systems and those who set up accounts.

Servers and data repositories are regularly maintained and patched using change management best practices and are secured with a full anti-malware strategy. There are policies in place to ensure that removable media is used in an authorized manner and is fully encrypted.

Data backups are carried out nightly and secured offsite in an encrypted manner with a recognized and bonded vendor. Logs are kept of the inventory of tapes.

All data transmitted is encrypted according to Advanced Encryption Standard (AES) using triple DES encryption.

ERS, Inc has started the process of risk assessments using industry standard tools and external consultants to ensure that the controls in place are adequate and vulnerabilities that can be exploited by a threat agent are identified and mitigated.

ERS utilizes an incident response system in place that monitors and responds to incidents involving the critical systems housing and processing confidential data as described in question one of this document.

ERS no. is currently re-writing the Information Systems Security Plan (ISSP) that details the security requirements and describes the security controls that are in place to meet those requirements. A certification and accreditation process in accordance with the National Institute of Standards & Technology (NIST) "Guide for the Security Certification and Accreditation of Federal Information Systems" will validate our security controls.

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

A "System of Records" was created for the Common Services for Borrowers (CSB) Contract. Enterprise Recovery Systems, Inc. is working under this "System of Records."

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