



START HERE
GO FURTHER
FEDERAL STUDENT AID

**Privacy Impact Assessment for
Coast Account Receivables Database (CARD)**

Date

March 18, 2009

Contact Point

Business Owner: Everett Stagg, President and Brian Davis, CEO

System Owner: Brian Davis, CEO

Author: Sylisa Freiburger, Information Systems Manager

Coast Professional, Inc.

1. What information will be collected for the system?

- Information of individual users collected
- Full name
- Date of birth
- Address
- SSN
- Phone
- Employment information
- Borrower Reference information (name, address, phone)
- School attended
- Checking account information
- Credit card information
- Banking information
- Collected correspondence
- Borrower account information (disbursement amount, principal balance, interest accrual, loan status, repayment plan, repayment amount, forbearance status, deferment status, separation grace period and delinquency)

2. Why is this information being collected?

- To aid in the collection efforts and resolve defaulted federal student loan accounts
- Federal and private institutional debt
- Coast Account Receivables Database (CARD) provides a vehicle for the storage, retrieval, and editing of borrower information
- Correspondence to the borrowers from Coast is provided by this system and on behalf of ED

3. How will Coast use this information?

Information obtained will be used to facilitate the collection and resolution of defaulted federal student loan accounts. CARD provides a vehicle for the storage, retrieval, and editing of borrower information and uses the information to collect defaulted federal student loan accounts. Information may be collected as part of the processing, collection, disposition, and resolution of the account.

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

Yes. In addition to the Department of Education having full access to all borrower information stored within CARD, limited borrower information will be shared with the following organizations upon compliance and approval with all FISMA/NIST requirements:

- Account Control Technology (PCA Mentor)
- National Credit Bureaus (vendors)
- Dolan (vendor)
- TALX (vendor)
- Lexis Nexis (vendor)
- CompuMail (vendor)
- VeriFacts (vendor)

5. Describe the notice or an opportunity 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 Coast Professional, 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 Coast Professional, Inc. receives 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 Coast Professional, 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. Coast Professional, Inc. company privacy policy also restricts the sharing of information.

6. How will the information be secured?

CARD has been secured at the physical, operating system, database, and network infrastructure security levels. The network complies with the security controls and procedures described in the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Special Publications, and Federal Information Processing Standards (FIPS). Please refer to the CARD System Security Plan (SSP) for the specific management, operational, and technical security controls deployed on the system. The SSP details how the following security control families are implemented on the system:

- Risk assessment
- Planning
- System and services acquisition
- Certification, accreditation, and security assessments
- Personnel security
- Physical and environmental security
- Contingency planning
- Configuration management
- Maintenance
- System and Information integrity
- Media protection
- Incident response
- Awareness and training
- Identification and authentication
- Access control
- Audit and accountability
- System and communication protection

Some specific security controls in place include:

- Operating systems and infrastructure devices are hardened in accordance with NIST moderate confidentiality controls.
- Vulnerability scans are conducted periodically to ensure supporting systems and all applications are at the highest state of security and are patched accordingly. Redundant firewalls are placed at entry points to the network with hardened access control lists.
- Intrusion detection systems are in place to spot any malicious activity.
- Least privilege policy is practiced throughout the organization.

In addition, CARD identifies authorized users of the information system and specifies access rights/privileges. CARD grants access to the information system based on:

- (i) a valid need-to-know basis that is determined by assigned official duties and satisfying all personnel security criteria;
- (ii) intended system usage.

CARD requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. CARD ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know changes.

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. Coast Professional, 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).