Privacy Impact Assessment
for
Diversified Collection Services, Inc.
US Department of Education Collection System

Date

March 18, 2009

Contact Point

System Owner: **Hal Leach, President DCS**

Author: **Bruce Mackinlay, IT Director**

1. What information will be collected for the system?

Diversified Collection Services' (DCS) primary business is to act as a collections agent for the Department of Education (ED). As their agent, we contact borrowers and collect on defaulted debts. The following information on individual borrowers will be collected:

- Full name
- Address
- Social security number (SSN)
- Phone number
- Email address
  Employment information

The following borrower information may also be collected:

- Disbursement amount
- Principal balance
- Interest accrual
- Loan status
- Repayment plan
- Repayment amount
- Forbearance status
- Deferment status
- Separation date
- Grace period and delinquency
- Personal credit card information
- Private health information (PHI)

2. Why is this information being collected?

DCS contracts with ED, Federal Student Aid (FSA) as a provider of debt recovery services. The information collected in the system is required for DCS to track and recover outstanding loans.

3. How will FSA use this information?

DCS provides a vehicle for the storage, retrieval, and editing of borrower information and uses this information to collect on defaulted accounts. Information may be collected as part of the student loan application processing, collection, and disposition of the account.

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

Information provided by ED is used only for the purposes of collecting on defaulted student loans. Functions performed, and the entities used to perform these functions, are:

Function	Entity	Type of data
Credit Reports on Borrowers & other Tools used to Locate Borrowers	Confidential. *Can be provided as needed.*	SSN, Name, DOB
Electronic Directory Assistance	Confidential. *Can be provided as needed.*	Name, Address, Phone
Printing of Letters	Confidential. *Can be provided as needed.*	Name, Address, Balance, Account Number
AWG Processing	Confidential. *Can be provided as needed.*	SSN, Name, DOB, Address, Balance, Account Number & Transactions
Clients Interface Website	Confidential. *Can be provided as needed.*	All Borrower's Data
National Change of Address	Confidential. *Can be provided as needed.*	Name, Address
Employment Data Skip Trace	Confidential. *Can be provided as needed.*	SSN, Name, DOB & Address
Voice Broadcasting	Confidential. *Can be provided as needed.*	Name, Phone Number
Bankruptcy, Incarceration & Decease Scrubbing	Confidential. *Can be provided as needed.*	SSN, Name, DOB, Address
On-Line Payment Processing	Confidential. *Can be provided as needed.*	SSN, Name, Account Number & Account Balance
Historical Tape Storage	Confidential. *Can be provided as needed.*	Completely Encrypted Backup Tapes

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.

A privacy notice displays on the DCS client website and states the following:

DISCLOSURE STATEMENT: "The user understands that the Department of Education, its agents and sub-contractors have agreed 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."

All other sessions have the following notice before the session is established (before the user logs in). On systems that can support a long text message, the following message is used:

"All Performant Financial Corporation computers are covered by federal & state privacy & security laws & regulations as covered in both the new-hire training and annual security awareness training:

- You may be accessing U.S. Government supplied information;
- Usage on this system may be monitored, recorded, and subject to audit;
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
- Use of the system indicates that you have completed security training and consent to monitoring and recording."

For systems that cannot support a long text message, the follow 128-character message is used:

"All Performant Financial Corporation computers are covered by federal & state privacy & security laws:

1. You may be accessing U.S. Government information;
2. Usage may be monitored and audited;
3. Unauthorized use of the system is prohibited;
4. Use of system indicates consent to monitoring and recording."

The DCS receives information from the Department of Education, Federal Student Aid Debt Management and Collection System (DMCS). As DCMS is the parent system from where DCS 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 DCS 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. DCS company privacy policy also restricts the sharing of information.

6. How will the information be secured?

DCS' procedures are fully compliant with Fair Debt Collection Practices Act (FDCPA), Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA) and other federal and state regulations. They are also aligned with Government Privacy Requirements as defined by the Department of the Treasury, the Department of Education, Health and Human Services and State Taxing Authorities.

DCS takes data communications security seriously. At the perimeter of the data communications network, dual Juniper® firewalls are used in a High-availability (HA) configuration at each Internet-facing site. The HA firewalls are implemented in the Livermore, CA and Grants Pass, OR data centers. The small network between the two firewalls is called the Demilitarized Zone (DMZ). Users accessing from outside can only communicate to servers within the DMZ. The firewall strictly regulates how those outside of DCS' network can use these servers. When users want to gain access to account information, they will pass through both the outer firewall and the inner firewall. To do this, users must communicate with a server sitting between the two firewalls in the DMZ. To gain access to this server, a user must have a SecurID card and log in through a Virtual Private Network (VPN). The VPN will only allow clients to communicate to a server in the DMZ using Triple-DES data encryption. Triple-DES is the national Data Encryption Standard for data communications as recommended by the National Institute of Standards and Technology. As a result, any communications between clients and DCS will be safe, private, and guaranteed to be limited to authorized personnel only.

The outer firewall only allows access to a server located between the two firewalls in the DMZ. By design, this server does not hold any information but acts as an intermediary during communications. Accessing the server is only allowed via the web and only from a specific IP address. As a result, only clients granted access by DCS can connect to this server. The web server also requires a user ID and password that restricts all access based on the identity of the user that logs into the server. The login also restricts access to specific account information that the user is authorized to access.

The user ID and password are not stored in the DMZ but are stored within the inner firewall on a highly secure authorization server. The web server inside the DMZ communicates across the second inner firewall only by the program that controls the access, and only to specific servers, using limited protocols. As a result, even if someone breached the outer firewall, they would be held within the DMZ and could not communicate with the inner firewall. This configuration of these two firewalls, and a limited server between the firewalls that contains no data, is considered the safest way to allow external users to gain access to a high-security system.

Along with the web server that is used to provide access to account data, DCS also has an email server in the DMZ. All emails from clients go to this email server. This email server contains the industry's best tools for scrubbing email for unwanted data and programs. All email is passed though McAfee VirusScan® for viruses, and a ProofPoint appliance to stop spam. DCS updates the virus scan and malware protections continuously so that viruses, malware, unwanted email, web content, and malicious programs are blocked at this email server before unwanted files enter the system.

In addition, each personal computer and server is set up with full security, including anti-virus software and password-protected screen savers that activate automatically. A constant security problem for computer users is the threat posed by computer viruses. To protect against the possibility of software viruses, all current operating software is carefully screened, and tight control is maintained over the acquisition of new software. Anti-virus software is installed on all company PC workstations and servers. Anti-virus software is also used on DCS' email server to scan files attached to emails before they are delivered to the recipient. The virus protection program monitors and controls software viruses on the entire system, eliminating the danger of corrupted files. This program is updated with new virus detection files on a regular basis or as new detection file updates are released.

DCS has a history of undergoing risk assessments and security reviews. These include a review by the Department of the Treasury based on the NIST 800-53 (rev 2) in November of 2007, a third-party independent, enterprise-wide, risk assessment performed in April of 2008 and an enterprise-wide SAS-70 Type II completed in November of 2008. DCS has employed an office of security, and a single individual responsible for security from 2005 forward. Security is a significant focus of DCS and is supported by the CEO and all branches of the organization.

Finally, the DCS system is currently undergoing a Certification and Accreditation (C&A) effort to ensure that Department of Education and FISMA compliant security controls are implemented. The anticipated completion of this C&A effort is October 2009.

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. DCS 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).

8. **List the web addresses (known or planned) that will have a Privacy Notice.**

1. www.dcsquickpay.com
2. www.dcsclient.com