START HERE
GO FURTHER
FEDERAL STUDENT AID

Privacy Impact Assessment
for the
Van Ru Collection System

Date
2/20/09

Contact Point
System Owner: James Lincoln, Contract Administrator AG568
Author: Maxine Sheinin, Information Security Manager

1. What information will be collected for the system?

Below are the fields from the EFT File Specification Document # **D-CAR-001-E** version 1.07 detailing all of the specific information received from the Department of Education and used for Van Ru's collection activities. In addition, Van Ru collectors update incorrect information and collect payment information for the repayment of loans.

Fields include: Account Region Code, Collection Agency Location Code, Account Type, Account Number, Last Name, First Name, Middle Name, City, State, Zip Code, Home Phone, Work Phone, Payment Due Date, Payment Amount, Stop Bill Flag.

2. Why is this information being collected?

Van Ru's AS400 Collection System provides the collector interface for the purpose of storing, retrieving and updating debtor information. Payments on defaulted accounts are processed by the Department of Education. All information collected is for the sole purpose of contacting the consumer to resolve accounts owed to the Department of Education.

In addition, this system provides the information needed to produce official correspondence to debtors from ED.

3. How will FSA use this information?

FSA uses this information to update their records to reflect current consumer information, payment history and updated loan encumbrances.

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

Comment [m1]: This must be expanded or deleted based on Thursdays meeting to include RGS or not.

Comment [m2]:

- Information specific to skip tracing is shared with third-party vendors for the purpose of updating contact information. In order for Van Ru to accredit a third party, contract inclusions must include non-disclosure, an annual security review and compliance with Van Ru security policies as documented in the Third Party Security Handbook. Security reviews of third party operations are performed annually.
- Information needed to process letters to the consumer for legal compliance is shared with third-party letter production vendors. Van Ru applies the same security requirements to letter vendors as third party skip tracing resources.

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 Van Ru Credit Corporation login banner is displayed and must be agreed to before the login screen appears. The statement is as follows:

> "This machine, and the software used in connection with it, is to be accessed and used only by employees, and only in connection with the conduct of the business, of Van Ru Credit Corporation. This machine is the property of Van Ru and you will be held responsible for any damage to or destruction of it. All software used in connection with this machine either is owned by or licensed to Van Ru.
>
> You may not copy all or any part of any such software. You may not use or load onto this machine (including internet downloading) any other software.
>
> In addition, all information accessed through this machine either is confidential and/or proprietary to Van Ru or to its clients. All such information must be held in confidence and

may not be used or disclosed except as necessary in the furtherance of Van Ru's business.

Any violation of the above, as further explained in the Employee Manual, will subject you to disciplinary action up to and including termination of your employment as well as potential civil and/or criminal liability.

By clicking OK and logging on to this computer you acknowledge the above and reaffirm your agreement to adhere to the policies and procedures as stated in this message as well as those stated in the Van Ru Credit Corporation Information Acceptable Use Policy."

Additionally, employees and contractors must sign non-disclosure agreements regarding privacy prior to obtaining access to client information.

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

6. How will the information be secured?

Van Ru's approach to protecting sensitive data involves protection against the intentional and accidental misuse of its paper and electronic data, including data concerning Van Ru's personnel and organization, and its clients' information. Van Ru is committed to handling ED information with the highest standards of information security including:

- Encrypting all Personally Identifiable Information (PII) at rest and in transit
- Restricting access of PII to employees on a "need to know" basis
- Maintaining physical, electronic, and procedural safeguards to meet federal regulations and industry best practices
- Reviewing and assessing information systems and processes regularly to ensure integrity and security at all times
- Requiring all third-party providers adhere to Van Ru's standards to keep customer/borrower information safe and secure

Van Ru's Information Security Department reviews and audits compliancy with policies and procedures in place to limit risk in the areas of physical access, logical access, and compliance with industry security standards and governmental regulations. Approved policies and updates to these policies are communicated through training, postings to Van Ru's intranet security website, email, and newsletter articles. All security policies and standards are outlined in Van Ru's *Organizational Security Policy*.

Awareness and Training - New employees must attend training on Van Ru's legal responsibilities including FISMA, FDCPA, GLB, FACTA and BSA among other regulations. All employees receive Security Awareness training on an annual basis and must pass a required test to ensure understanding.

Van Ru's Security Center, an intranet Website accessible through every employee's workstation, contains a constant stream of updated information to support a proactive and compliance-driven working environment. This information includes, but is not limited to, the following:

- State-specific regulations (an easy to use state-by-state guide highlighting varying regulations)
- Security policies covering all 17 families of security controls as dictated by NIST's Federal Information Systems standards
- Security Trends (identity theft, phishing, pretexting, etc.)
- FDCPA, FACTA, and GLB requirements
- Links to training materials and exams

Physical Security - An electronic badge entry system controls, monitors, and logs access to Van Ru's secure areas and is programmed to regulate such access based on job requirement. To facilitate visitor control, all non-employees are required to sign-in and are escorted throughout the duration of their stay. The following table lists the physical security features in place at all Van Ru facilities and data centers.

Security Control	Benefit
Electronic Card Readers	Provides an audit trail and limits access based on job requirement
Closed Circuit TVs (CCTV)	Monitors and records activity on collection floors and accounting areas as well as entrances to secure areas
Electronic Alarm System	Notifies alarm service company of intrusion and other threats
Visitor Log and Non-disclosure Statement	Records activity and promotes confidentiality
Disabled Peripheral Devices & Internet ports	Peripheral devices (e.g. CD-ROM, printers, etc.) as well as unused Internet ports are disabled in order to prevent the removal of electronic/hard copy data
Data Center Security	▪ Restricts access to Data Center through a 2-factor authentication process (keypad and card reader) ▪ Data Center is protected by glass breakage, water detection and fire suppression systems ▪ Redundant back-up data center is maintained offsite
Door Alarms	Alarm triggers if door is held open for more than 60 seconds

Media Protection - The process for handling correspondence and other non-electronic information pertaining to client records assures the safe and proper disposal of sensitive material. A process to log, track, scan and dispose of sensitive correspondence is in place at all Van Ru locations. Document imaging is used to archive paper documents and is access-controlled to permit authorized users only. During disposal, non-electronic data containing sensitive or personal information is collected and shredded onsite through the use of an outside vendor who adheres to Van Ru's documented third party standards. Following is a summary of the methods by which Van Ru handles various types of media:

- Portable Media No Longer In Use - Backup tapes are reused. Failed backup tapes are removed from their case and shredded. CD-ROMs, floppy diskettes and other removable media are removed from their cases and shredded. Before disposal of removable media (including but not limited to hard drives), the media is “wiped” using four (4) passes of strong random data followed by one (1) pass of zeros with reverse wiping direction enabled.
- Non-Failed Media - Media that contains company confidential information or client-delivered data is handled as follows:
  - If client process requires return of said media, a tracked system of returning media is used.
  - If client process requires disposal of media, the process is to “wipe” the media using four (4) passes of strong random data followed by 1 pass of zeros with reverse wiping direction enabled, a standard acceptable by DOD security standards.
- Failed Media - Failed media is removed from component parts and destroyed using Degaussing technology.
- Redistribution of Desktop Computers - Computers re-imaged for purposes of re-use or redistribution are required to be wiped as described above.

Identification and Authentication - Van Ru utilizes a secured VPN for employees and clients to authenticate access to approved systems. Encryption, authentication headers and key re-negotiation are utilized for data transmitted across the VPN. It is Van Ru’s policy to prohibit connectivity by any outside system other than client-owned, managed and approved systems.

Risk Assessment - Van Ru uses a comprehensive, self-directed, information security risk evaluation as a systematic, organization-wide approach to identify and prioritize risks. These internal risk assessments, along with annual independent audits and network vulnerability scans, represent the foundation of information security risk management at Van Ru. An evaluation to assess mitigation efforts documented in the previous assessment is scheduled annually. This review of current practices compared to documented policies and safeguards is crucial to maintaining ongoing security and privacy of client information.

Access Control - Van Ru believes in a multi-layered approach to security or a Defense-in-Depth strategy. To ensure the security of the data resident on Van Ru’s systems, all users have controlled access to system tasks by means of network group security. Van Ru assigns unique User IDs and requires strong passwords that expire every 60 days. Access to applications is based on job requirement and uses a menu-driven system to restrict access. Users are given permission to access only those menu-items (applications) that are necessary to fulfill their assigned duties.

Additionally, Van Ru adheres to a written Incident Handling and Reporting process in place to deal with any reported breach to security policies.

System and Communication Protection - Van Ru requires the encryption of outgoing data sent via the Internet, either at the transmission level using an SSH or SSL based protocol, or at the file level using encryption software such as PGP or WinZip. Van Ru prohibits the use of any wireless communication devices. Modems may not be directly connected to a networked workstation, and analog lines are only designated for fax machines and stand-alone computer systems with a documented business requirement.

For email communications, Van Ru uses Microsoft Exchange Server 2003 with a forward facing, segregated SMTP server. Van Ru’s policy requires encryption of all non-public information sent outside the company. For remote access, Van Ru’s VPN tunneling implementation uses IPSEC, 3DES and SHA encryption.

For data control and WAN traffic, we have a physical De-Militarized Zone protected by redundant Cisco firewalls, which are set to deny all traffic not expressly permitted. Van Ru's internal network environment further layers access through switches and routers using VLANs to segregate and separate operational areas. Our critical applications, aside from being on a separate segment, are protected internally by an additional set of redundant Cisco firewalls. In total, Van Ru utilizes seven (7) firewall sets with automatic failover. Branch locations on the wide-area network are connected using a Global Crossing MPLS or IP/VPN. These connections are either encrypted or utilize pre-defined Permanent Virtual Circuits.

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. Van Ru Credit Corporation 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).