Privacy Impact Assessment
for the
Private Collection Agency Premiere Credit

Date
March 15, 2009

Contact Point
System Owner: JD Mabbitt
Business Owners: Dave Hoeft & Todd Wolfe
Primary Application Owner: Todd Wolfe
Author: JD Mabbitt

1. What information will be collected for the system?

1. Borrower Full Name
2. Borrower Address Information
3. Borrower Social Security Number
4. Borrower Phone Numbers (home, work, cell)
5. Borrower Email Address
6. Borrower Employment Information
7. Borrower information to include: loan information, repayment terms, payment history, disbursement amount, principal balance, interest accrual, loan status, forbearance status, deferment status, separation date, grace period, delinquency, and incarceration status.

2. Why is this information being collected?

All information received from the Department of Education is used for the sole purpose of contacting the consumer and collecting owed funds on behalf of the Department of Education. Premiere Credit will utilize the information to (1) Make contact with the debtor, (2) Collect outstanding debt, and (3) Qualify debtor for rehabilitation or resolution.

3. How will the Department of Education use this information?

The Department of Education uses this information to update their records with current consumer information, payment history and updated loan encumbrances. Premiere Credit will use this and all other information obtained to support the collection of defaulted student loans for the Department of Education. Information is used for skip-tracing, location, collections, repayment and rehabilitation monitoring, and reporting results to the Department of Education.

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

Yes; information collected will be shared with the following companies:

1. Experian – for disability status
2. CompuMail – a letter processing vender
3. Accurint – skip-tracing
4. Central Research – skip-tracing
5. TeleTrak – skip-tracing
6. Lexus-Nexus – bankruptcy and death verification

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

1. All letters, emails, and faxes sent to borrowers contain FDCPA and State mandated disclosures regarding the use of information obtained for the purpose of debt collection.
2. Every debtor call is initiated with a Miranda statement disclosing the purpose of the call is to collect a debt and that any information provided will be used for that purpose.
3. Premiere Credit does not place disclosure notices on its commercial website. Borrowers are not directed to this site, no payment arrangements may be entered, no borrower account information is accessible from this site, and no collection effort is initiated from this site. The website is used for client access and applicant recruitment.

6. How will the information be secured?

1. Access to Premiere Credit's facilities is protected by 24 hour video surveillance. The building is secured with a perimeter alarm and internal motion detectors and video surveillance. Only top level management has the ability to disarm the alarm. Employee access is controlled and monitored via a security fob assigned to them at hire; the fob is required to gain or regain access to the building.
2. Access to Premiere Credit's computer system is controlled by user name and password.
3. Access to the FACS application is limited to authorized individuals who have been granted an application user name and password.
4. All Department of Education borrower accounts are kept in a collection directory totally separate from other client accounts. No Department of Education account can be accessed except by authorized Department of Education approved staff person.
5. Premiere Credit provides extensive new hire training, which covers information security. This training is refreshed annually. All users are required to read and follow Premiere Credit's and the Department of Education's information security rules and regulations – each employee is required to sign a statement acknowledging the regulations and affirming they will follow the regulations.
6. Access to the Department of Education collection floor is restricted to authorized personnel only; staff, including management, which have not been cleared to access Department of Education information are not allowed in this restricted area.
7. Outbound vender files and emails containing privacy information are encrypted.
8. Access to the IT work area is restricted by a finger-print scanner; this area is also zone-alarmed separately from the general building alarm system. Within the IT work area, access to the secure server room is controlled by a bio-metric hand scanner; this area is also separately zone-alarmed, with a 15 minute duration reset, and motion detectors to prevent unauthorized access. The server room is also under 24 / 7 video surveillance.
9. In addition to the controls outlined above, Premiere Credit undergoes an independent Security Authorization process every three years utilizing the requirements set forth by the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and the 800 series of Special Publications.

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

[*Response to question 7 will be provided by the Department of Education*]