

Exhibit B
Security Certificate

Simpluris Security Summary – White Paper

Simpluris is committed to the security and overall protection of not only our data and information but our client's data and information, as well. As a demonstration of our commitment, we maintain SOC 2 Certification which requires strict adherence to policies and procedures surrounding information security, including processing and storage of confidential customer data. Simpluris supports a comprehensive, written Information Security Program that complies with all applicable laws and regulations (e.g. HIPAA, Gramm-Leach-Bliley Act, MA 201 CMR 17.00) and is designed to (a) ensure the security, privacy and confidentiality of Client and Class Member Information, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of Client or Class Member Information, and (c) protect against unauthorized access to, use, deletion, or modification of Class Member Information. Simpluris has designated specific employees to be responsible for the administration of its Information Security Program. Also, Simpluris regularly and routinely monitors, tests, and updates our Information Security Program.

Simpluris uses Client and Class Member Information only for the purposes for which its' clients provide it, as described in any Agreements or Court Orders governing the provision of Simpluris' services in any particular case. Simpluris maintains a process for identifying, assessing, and mitigating the risks to Class Member Information in each relevant area of Simpluris' operations. At Simpluris, we continuously evaluate the effectiveness of the safeguards for controlling these risks to data and bank accounts. Simpluris restricts access to Class Member Information only to those employees, agents, or subcontractors who need to know the information to perform their jobs. Simpluris performs background checks of all its employees that will have access to Sensitive Personal Information, including a review of their references, employment eligibility, education, and criminal history to ensure they do not pose a risk to the security of Client or Class Member Information.

Simpluris adheres to the following industry best practices to safeguard its systems which process, store or transmit Client and Class Member Information:

- Identity and Access Management;
- Complex passwords are routinely and regularly changed;
- Role-based access control systems to limit individual employee access to network applications and systems based on their particular job role and function;
- Data Loss Prevention and Intrusion Prevention System software at multiple layers to prevent from internal and external threats of data leaks, malicious activity, and policy violations
- Encryption of Class Member Information if transmitted over public or wireless networks (e.g., via email, FTP, the Internet, etc.);
- Implementation of a Secure File Transfer system (using SSL encryption) for transmitting documents back and forth to clients;
- Encryption of servers, portable media, laptops, desktops, smartphones, mobile devices, and new technologies that store Class Member Information;
- Complex password authentication for remote access to Company's networks;
- Upon hire and annually after that, training of all employees with access to Class Member Information, (including any agents, and subcontractors with access to Class Member Information) about their obligations to implement the Information Security Program;
- Strict disciplinary measures for employees who violate the Information Security Program;
- Preventing terminated employees from accessing Class Member Information;
- Appropriately configured and updated firewall, antivirus, and spyware software;
- Prompt application of vendor-recommended security patches and updates to systems and other applications to avoid any adverse impact on Class Member Information;
- Separation of Duties;
- Infrastructure and Physical Security;
- Business Continuity Planning;
- Disaster Recovery Planning