PROOF SECURITY STATEMENT

Capitalized terms not otherwise defined have the meanings given in Proof General Terms ("**General Terms**") or the Proof Glossary.

1. Information Security Controls. Proof has implemented and will maintain reasonable technical, physical and organizational measures that meet or exceed legal requirements and frameworks in compliance with applicable law intended to protect User Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

2. Frameworks, Compliance, and Audits.

2.1 Frameworks. Proof's security program includes controls that meet the requirements of the:

(a) American Institute of Certified Public Accountants ("**AICPA**") Trust Services Criteria, as validated by annual SOC2 audits and the resulting reports;

(b) National Institute of Standards and Technology ("**NIST**") Special Publication 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations," at the moderate level and related security requirements contained in NIST Special Publication 800-63A, at the Identity Assurance Level 2 ("**IAL2**"), as validated by annual audits;

(c) WebTrust Principles and Criteria For Registration Authorities, as validated by annual audits;

(d) 201 Code of Massachusetts Regulations ("**CMR**") 17.00, Standards for the protection of personal information of residents of the Commonwealth, as documented in Proof's Written Information Security Policy; and

(e) The Payment Card Industry ("**PCI**") controls applicable to e-commerce merchants who outsource all payment processing to PCI Data Security Standards ("**PCI DSS**") validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises as validated by annual completion of Self-Assessment Questionnaire ("**SAQ**") A.

2.2 Additional Legal Requirements. Based on Proof's controls as implemented under the previously listed frameworks and legal requirements, Proof also meets:

(a) Health Insurance Portability and Accountability Act ("**HIPAA**") requirements applicable to Business Associates as defined in HIPAA;

(b) Family Educational Rights and Privacy Act ("**FERPA**") requirements applicable under the "School Official" requirements and relevant guidance from the Department of Education;

(c) Gramm Leach Bliley requirements applicable to Service Providers as defined in Gramm Leach Bliley; and

(d) NIST Special Publication 800-171 Revision 2.

3. Security Incidents.

3.1 Incident Response Plan. Proof maintains a cyber-incident breach response plan in accordance with Proof's Written Information Security Policy ("**Incident Response Plan**") and implements the procedures required under such plan on the occurrence of a Security Incident.

3.2 Security Incident Notification. If Proof becomes aware of a Security Incident, Proof, after initial investigation, without unreasonable delay: (1) provides a notification of the Security Incident that will be delivered to one or more of Subscriber's administrators by email ; (2) investigates the Security Incident and, after completing its investigation, provides Subscriber with information about the Security Incident; (3) uses reasonable efforts to mitigate the effects and to minimize any damage resulting from the Security Incident and, after doing so, informs Subscriber of the steps taken; and (4) once determined,

informs Subscriber of any modifications Proof makes to its security procedures that are intended to prevent similar security incidents occurring in the future.

3.3 Information Security Incident Management.

(a) *Incident Response Process*. Proof maintains a record of Security Incidents with a description of the Security Incident, the time period, the consequences of the incident, the name of the reporting person, to whom the Security Incident was reported, and the procedure for recovering any affected data. Proof shall track Security Incidents, including what data has been disclosed and to whom, or what data has been lost, damaged, destroyed or altered (as the case may be), and at what time.

(b) *Service Monitoring*. Following a Security Incident, Proof security personnel review relevant service-related logs to propose remediation efforts, if necessary.

* * * * *