

	Security Review Questionnaire Crescendo's Cloud-Based Planned Giving Software
<p>Prepared By: Crescendo Interactive, Inc.</p> <p>Effective Date: September 7, 2018</p> <p>Crescendo Contact Information: Crescendo Interactive 110 Camino Ruiz Camarillo, CA 93012 Phone: 800-858-9154 Web: crescendointeractive.com</p>	<p>Application of Information: The information contained in this Security Review Questionnaire ("SRQ") is related solely to the following cloud-based planned giving software products offered by Crescendo: CresPro, CresEstate and CresLite (collectively "Crescendo Software"). This information is current as of the Effective Date. This SRQ does not apply to other products offered by Crescendo (such as our CD-based software) and certain explanations may change if Crescendo Software is used in conjunction with other services (such as our GiftLegacy or GiftLaw marketing services).</p>

1. Background and Other Key Information.

1.1 About Crescendo. Crescendo Interactive, Inc. (hereafter "Crescendo") started more than over 30 years ago. We are the only full-service planned gifts marketing company. In addition to offering donor illustration software, such as the Crescendo Software, we also offer a full complement of planned gifts marketing services including applications for web, email, print, social media, multimedia, training and support. We have developed and support our products fully in house. A majority of organizations choose Crescendo not only because of our rich history of innovative and trend setting services, but also for our excellent customer support.

1.2 About the Crescendo Software. Crescendo Software is cloud-based. Each of the three software products that are included within Crescendo Software (CresPro, CresEstate and CresLite) are hosted on and accessible by way of the website, CresManager.com. Each software product includes different program offerings to calculate different major, blended and planned gift options. A current list of the individual programs included with each product is available for review on Crescendo's website, crescendointeractive.com.

1.3 Definitions. In this SRQ, certain terms have special meaning and those terms are defined below.

1.3.1 Agreement - Refers to the Crescendo Software License Agreement (which may also be referred to herein as the "CSLA" or "EULA"). The Agreements is a click-wrap agreement meaning that a Registered and Licensed User must affirmatively acknowledge and agree to the terms of the Agreement, presented in an online format, prior to using the Crescendo Software.

1.3.2 Crescendo - Refers to Crescendo Interactive, Inc., a California corporation with an address of 110 Camino Ruiz, Camarillo, CA 93012. Crescendo has developed, owns and retains all rights of ownership and control related to the Crescendo Software, subject to a grant of rights to Licensee as stated in the CSLA.

1.3.3 Crescendo Software - Refers to CresPro, CresEstate and CresLite software together with any accompanying and associated media, and printed materials packaged therewith. Crescendo Software is cloud-based software available at the CresManager.

1.3.4 Crescendo Software Purpose - Refers to the use of the Crescendo Software by a Registered and Licensed User of the software, typically a member of the fundraising staff at a 501(c)(3) tax-exempt, non-profit or a professional advisor, such as an attorney, CPA or financial advisor, to prepare major, blended and planned gifts illustrations to encourage a donor or prospective donor to make a charitable gift by detailing the specific tax and other benefits.

1.3.5 CresManager - Refers to the website www.cresmanager.com, which is a secure, password-protected, software portal used to access and operate the Crescendo Software. CresManager access requires a Registered and Licensed User to enter a unique username and password. SSL is used throughout the CresManager.

1.3.6 License - Refers to the grant of a single seat, non-exclusive, annual license permitting Licensee (and only Licensee) to use the Crescendo Software subject to the terms of the EULA.

1.3.7 Licensee - Refers to the single, individual user of the Crescendo Software who must, prior to using the Crescendo Software, agree to the EULA and be a Registered and Licensed User.

1.3.8 Registered and Licensed User - Refers to an individual (not a corporation or business entity) who: (1) has contacted Crescendo and provided the individual's name, business address and other information requested by Crescendo to register as a Licensee; (2) has paid all applicable annual or other licensing fees to Crescendo; and (3) is recognized and authorized by Crescendo to use the Crescendo Software. Individuals who are not Registered and Licensed Users are not permitted to use Crescendo Software.

1.3.9 Seat License - Refers to the fact that the EULA permits Licensee, and only Licensee, to use the Crescendo Software. As a seat licensee, Licensee is permitted to use the Crescendo Software on a total of up to two registered devices (such as a work computer, work laptop, personal laptop or tablet computer) provided both are under the exclusive control of the Licensee and Licensee does not allow anyone else to use the Crescendo Software on those devices.

1.3.10 Subscriber - Refers to one or more of the following (as applicable): (1) the organization that Licensee has listed as its employer when registering as a Registered and Licensed User; (2) the organization that sponsors a License by either authorizing use of the Crescendo Software and/or paying the applicable licensing fees on behalf of Licensee; and/or (3) an organization that has a current, valid and paid license to use Crescendo's GiftLegacy marketing service which includes up to two (2) complimentary Crescendo Software Licenses for individuals who are employees of Subscriber and who Subscriber has indicated should be Registered and Licensed Users.

2. Interaction with Information Protected by Privacy Statutes.

2.1 - Is the Crescendo software designed to save/retain any of the following information protected by law:

2.1.1 Personal Information/Personally Identifiable Information?

Answer: No

Explanation: The Crescendo Software is not designed to save, retain or manage information that would be considered Personal Information (or Personally Identifiable Information) under applicable state law.¹

2.1.2 Payment Card Industry ("PCI") protected information?

Answer: No

Explanation: Payment Card Industry Data Security Standard ("PCI DSS") is a set of standards applicable to transactions where a company accepts, processes, stores or transmits credit card information and requiring that payment processing occur in a secure environment. Crescendo Software does not use or interact with credit card or other payment methods and the Crescendo Software is not a payment processing system. Accordingly, there are no PCI implications related to use of the Crescendo Software.

2.1.3 Information (including "PHI") protected under HIPAA?

Answer: No

Explanation: Federal law protects: (a) individually identifiable health information; and (b) protected health information ("PHI"). It is not uncommon for development staff at a hospital or other "Covered Entity" defined by HIPAA to use the Crescendo Software consistent with the Crescendo Software Purpose. The federal government has issued a "final rule" excluding fundraising information from HIPAA if the Covered Entity complies with the final rule, in which case, the Crescendo Software would not retain information protected by HIPAA.²

2.1.4 Student Privacy under FERPA?

Answer: No

Explanation: The Family Educational and Privacy Act (or "FERPA") is a federal law that protects the privacy of student education records. FERPA applies to schools that receive federal monies from the U.S. Department of Education. The development and fundraising staff of many universities, colleges and other schools across the United States, which are subject to FERPA, (individually an "educational institution") use the Crescendo Software consistent with the Crescendo Software's Purpose. According to the U.S. Department of Education regulations, fundraising-related information (such as a prospective donor's name and date of birth) is not protected by FERPA.

¹ Applicable state law is defined in the CLSA as California law, Civil Code Section 1798.82 which defines PI as either: (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number; (B) Driver's license number or California identification card number; (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (D) Medical information; and (E) Health insurance information - OR - (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account. Where: "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records; "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

² Federal Regulations provides guidance to Covered Entities, and supporting organizations such as a related charitable foundation, related to fundraising. You may wish to review those guidelines concurrently with this SRQ.

2.1.5 Non-Public Personal Information under Gramm-Leach-Bliley?

Answer: No

Explanation: The Gramm-Leach-Bliley Act ("GLBA") is a federal law enacted in 1999 to protect the security and confidentiality of "nonpublic personal information" ("NPI") of consumers. GLBA prohibits "financial institutions" from directly or indirectly disclosing NPI to non-affiliated third parties except in accordance with a published privacy policy. Financial institutions are required to provide annual privacy and opt-out notices to customers and consumers whose information would otherwise be disclosed. GLBA's privacy rule also affects "affiliates of financial institutions" and "nonaffiliated third parties." Given the construct of GLBA's privacy rule and related policies, GLBA does not apply to Crescendo or our services.

2.2 Does the Crescendo Software use any information identified in Section 2.1?

Answer: Limited Use

Explanation: In addition to preparing donor illustrations, Crescendo Software can be used to create certain documents associated with marketing, administering and closing blended, major and planned gifts. Examples of these documents include cover letters to donors summarizing an illustration, donor gift acknowledgments, notices required by the federal Philanthropy Protection Act, trust documents for non-revocable charitable trusts (such as charitable remainder unitrusts and charitable remainder annuity trusts) and charitable gift annuity ("CGA") agreements that comply with the requirements of each U.S. state.

A CGA is an agreement between a charity that has a license to issue, is registered to issue or is otherwise legally permitted to issue a CGA. CGA agreements are legally binding contracts where, in exchange for a gift from a donor, the issuing charity agrees to make lifetime, fixed payments to a beneficiary or beneficiaries selected by the donor (where the donor might also be a beneficiary). Most often, the state law that governs a given CGA is the law of the state where the donor resides (rather than the charity's state of incorporation or business location). Applicable law matters in terms of the legally required provisions of the CGA agreement, legal enforceability, and CGA reserve balance requirements and annual reporting. Certain states require, while others encourage, inclusion of each beneficiary's Social Security Number ("SSN") in the CGA agreement so as to identify, with certainty, who the beneficiaries are.

It is in this very limited context - the need to produce state-compliant CGA agreements - that a Registered and Licensed User of the Crescendo Software can input a beneficiary's SSN into the appropriate SSN data field of the software. In which case, the software will generate a state-compliant CGA agreement, in PDF format, in a new browser window/tab for the user to print on a printer, enabling the CGA agreement to be signed by the donor(s) and charity. For security purposes, however, the Crescendo Software includes the following safeguards: (1) the Crescendo Software does not save any SSNs when generating the PDF; (2) information inputted into a data field can be saved in the Crescendo Software to create or update a data record, however, information inputted into any SSN data field will NOT be saved as part of that data record; and (3) the Crescendo Software will only use the SSN during the current browser session (via "session cookies"). The Crescendo Software is specifically designed NOT to save SSNs in data fields designed for their use, even though use of SSNs is possible within the limited circumstances described herein for purposes of compliance with state law.

2.3 Has Crescendo addressed the EU'S General Data Protection Regulation (GDPR)?

Answer: Yes

Explanation: Crescendo has taken the following steps to address GDPR with respect to the Crescendo Software: (a) the CLSA was updated to include terms addressing GDPR and a current copy of the CLSA is available online at <https://www.crescendointeractive.com/terms/> (the "Terms Page"); (b) in May 2018, Crescendo gave Licensed and Registered Users notice of the changes to the CLSA in the form of a click-wrap agreement and any Licensed and Registered User who accessed the Crescendo Software since that time would have had to agree to these new terms prior to using the Crescendo Software; (c) the CLSA incorporates by reference terms of a certain "Data Processing Addendum" (or "DPA") which contains terms required by GDPR, including in relation to data processing and other matters, the DPA can also be found on the Terms Page; and (d) Crescendo has appointed designated staff to assist Subscriber with respect to any GDPR-related data subject inquiries, spelled out in the DPA the process by which Subscriber can request assistance.

3. Policies and Procedures.

3.1 Does Crescendo have in place policies and/or procedures covering the following:

3.1.1 Access Control?

Answer: Yes

3.1.2 Password Management?

Answer: Yes

3.1.3 Security-Related Incidence and Response Handling?

Answer: Yes

3.1.4 Data Handling (use, storage and destruction of sensitive information)?

Answer: Yes

3.2 Does Crescendo undertake regular reviews and update/revise policies as necessary?

Answer: Yes

- 3.3 Are senior Crescendo officials directly responsible for implementing organizational security?** Answer: Yes
- 3.4 Do Crescendo officials with network Admin privileges have individual access accounts?** Answer: Yes
- 3.5 Is the advice of an information security specialist obtained where appropriate?** Answer: Yes
- 3.6 Is the advice of Crescendo's legal counsel obtained where appropriate?** Answer: Yes
- 3.7 Are Crescendo's security roles and responsibilities clearly documented?** Answer: Yes
- 3.8 Do all Crescendo employees receive appropriate Information Security Training?** Answer: Yes
- 3.9 Does Crescendo apply security patches on a monthly or as-needed basis?** Answer: Yes
- 3.10 Are duties and areas of responsibility separated in order to reduce opportunities for unauthorized modification or misuse of information or services?** Answer: Yes
- 3.11 Does Crescendo validate modifications to the software, including patches?** Answer: Yes
Explanation: All development and testing is done in-house, in multiple layers and rounds of testing and has no impact on client data or operations. Minor fixes are only published live after they are deemed fit for production. Major releases and enhancements go through an additional round of testing on a private, production level test server (sandbox) that only houses unpublished code. This allows for use and testing in a production environment without the risk of breaking the Crescendo Software. Major upgrades that require a server reboot or other system downtime are done after hours, during scheduled maintenance periods or on weekends.
- 3.12 Does Crescendo collect and/or review log information related to the following:**
- 3.12.1 User access logs for the CresManager?** Answer: Yes
Explanation: Each login to CresManager is recorded as to User ID, Time and Date of Login and the IP address from which the login occurred. Changes and resources accessed are not logged.
 - 3.12.2 System logs for operation systems?** Answer: Yes
 - 3.12.3 Network devices such as firewalls, router and switches?** Answer: Yes
- 3.13 Does Crescendo Retain User Access Logs for a Specific Period of Time?** Answer: Yes
Explanation: Database archives, which include user access logs are kept indefinitely.
- 3.14 Does Crescendo employ regular monitoring to ensure recovery of key data?** Answer: Yes
Explanation: Disaster recovery systems are consistently monitored. These systems include database backup and replication and web server code backup and sync across production and mirror equipment. In the event of a total loss at our primary data center, mirror services could be up in an hour depending on DNS propagation time. Database content is backed up and archived on a nightly basis. Backup data is stored in the Crescendo office as well as offsite at the Primary Datacenter. In case of fire or complete destruction of the data center where we house our servers, disaster recovery plans are in place. We maintain a mirror network in another Arizona that can easily have traffic routed through it in the event of disaster or catastrophic failure.
- 3.15 Does Crescendo encrypt the following:**
- 3.15.1 Crescendo Software-related information, generally?** Answer: Yes
Explanation: Crescendo Software data is encrypted at rest using AES 128-bit encryption.
 - 3.15.2 First Name of any person saved as part of a software data record?** Answer: Yes
 - 3.15.3 Last Name of any person saved as part of a software data record?** Answer: Yes
 - 3.15.4 Date of Birth of any person saved as part of a software data record?** Answer: Yes
 - 3.15.5 Address of any person saved as part of a software data record?** Answer: Yes
- 3.16 Will any electronically-stored media that includes Subscriber data be securely cleaned, degaussed or destroyed prior to disposal?** Answer: Yes
- 3.17 In the event of a data breach, will Crescendo notify Subscriber?** Answer: Yes
Explanation: In the event that Crescendo confirms that any Crescendo server system on which Subscriber's confidential data is stored has been compromised by an actual data breach and that Subscriber data has been compromised (hereafter a "security incident"), then Crescendo will notify Subscriber within a commercially reasonable timeframe of the security incident after Crescendo has: (1) identified and remediated the source of the security incident; and (2) been able to determine which Subscriber data has been compromised, provided however, that notice is consistent with any guidance provided by or otherwise not prohibited by any law enforcement agency who has jurisdiction to investigate the security incident.

4. Password Security.

4.1 Is there a formal management process for issuing and resetting passwords?

Answer: Yes

Explanation: For CresManager password resets, an email is sent out to the user's email address with a temporary password. Logging in with a temporary password automatically triggers a password reset and a temporary password can only be used for a single login.

4.2 Can Crescendo recover forgotten passwords?

Answer: No

Explanation: Forgotten passwords are unrecoverable, even by Crescendo employees and must be reset if forgotten.

5. Physical and Network Security.

5.1 Is Crescendo's primary data center located in the United States?

Answer: Yes

5.2 Is this data center SOC-1 compliant?

Answer: Yes

5.3 Is the data center in a facility with 24-hour security, multiple internet connections, with redundant power supplies and does facility access require badge access, biometric confirmation access and lock and key access for anyone prior to accessing Crescendo's locked cage-type rack environment?

Answer: Yes

5.4 Does Crescendo have a back-up server system and is that located in the U.S.?

Answer: Yes

5.5 Is firewall technology in place to control data and service access?

Answer: Yes

5.6 Are there intrusion and prevention/detection systems in place?

Answer: Yes

5.7 Are there incident response processes in place?

Answer: Yes

6. Supported Devices and Software.

6.1 What hardware/software/connections are required to access the Crescendo Software?

Explanation: Crescendo Software is accessible via web-based portal on computers/tablets with general internet connection.

6.2 What devices does the Crescendo Software operate on?

Explanation: Crescendo Software operates on any PC, Mac or tablet device capable of running compatible web browsers.

6.3 As web-based software, what browsers are compatible with the Crescendo Software?

Explanation: Crescendo Software has been tested on Internet Explorer 11, Microsoft Edge, and current versions of Mozilla Firefox, Google Chrome and Safari.

7. Updates. Only the following persons are authorized to make updates and answer questions related to this SRQ, Zandro Diaz, Crescendo's Vice-President and Chief Technology Officer; Christopher Richardson, Crescendo's Assistant Vice-President and Information Technology Director or Christopher M. Jaarda, Crescendo's Senior Vice-President and Chief Legal Officer.

8. Approval. The information contained in this Security Review Questionnaire has been reviewed and believed to be true and accurate as of the Effective Date.

APPROVED: Christopher M. Jaarda
Senior Vice-President/Chief Legal Officer
Crescendo Interactive, Inc.

APPROVED: Christopher Richardson
Assistant Vice-President/IT Director
Crescendo Interactive, Inc.