DATA PRIVACY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE
AGREEMENT

1. Purpose

(a) This Data Privacy Agreement (DPA) supplements the agreement between Watervliet City Schools (THE DISTRICT) and Renaissance Learning, Inc. (Vendor), to ensure that the Vendor AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DPA Agreement, a copy of Watervliet City School District Parents Bill of Rights for Data Security and Privacy signed by Vendor and the Supplemental Information about the AGREEMENT that is required to be posted on district's website.

(b) To the extent that any terms contained within the Vendor AGREEMENT, or any terms contained within any other Agreements attached to and made a part of the Vendor AGREEMENT, conflict with the terms of this DPA, the terms of this DPA will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Vendor AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this DPA, the terms of this DPA will apply and be given effect.

2. Definitions

Any capitalized term used within this DPA that is also found in the Vendor AGREEMENT will have the same definition as contained within this DPA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from the district pursuant to the DPA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from the district pursuant to the Vendor AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from the district located across New York State, and that this Protected Data belongs to and is owned by the district from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and THE DISTRICT policy on data security and privacy. Vendor acknowledges that THE DISTRICT is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Vendor.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from the district in accordance with the district's Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by Vendor and is set forth below.

Additional elements of Vendor' Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this DPA, consistent with THE DISTRICT data security and privacy policy, Vendor will: See attached Information Security Overview.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Vendor AGREEMENT, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Vendor AGREEMENT: See attached Information Security Overview.

(c) Vendor will comply with all obligations set forth in THE DISTRICT "Supplemental Information about the AGREEMENT" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: See attached Information Security Overview.

(e) Vendor [*check one*] __x__ will ____ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Vendor AGREEMENT. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Vendor AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in THE DISTRICT "Supplemental Information about the Vendor AGREEMENT," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in THE DISTRICT "Supplemental Information about the AGREEMENT," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from the district, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the Vendor AGREEMENT and the terms of this Data Privacy Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the Vendor AGREEMENT.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the Vendor AGREEMENT, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the district no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in THE DISTRICT "Supplemental Information about the Vendor AGREEMENT," below.

(g) Provide notification to THE DISTRICT (to the extent required by, and in accordance with, Section 6 of this Data Privacy Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse THE DISTRICT, for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify THE DISTRICT of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has confirmed the breach or unauthorized release.

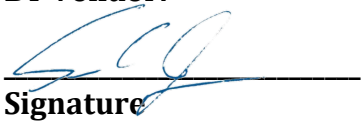
(b) Vendor will provide such notification to THE DISTRICT by contacting THE DISTRICT: Kirsten DeMento.

(c) Vendor will cooperate with THE DISTRICT and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the district affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, THE DISTRICT, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by THE DISTRICT, Vendor will promptly inform the Data Protection Officer or designees.

(e) Vendor will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to the DISTRICT or Regional Information Center.

BY Vendor:



Signature

Director, Security Ops & Compliance

Title

10-17-2024

Date

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

The Watervliet City School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

2) Parents have the right to inspect and review the complete contents of their child's education record.

3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4) A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5) Parents/guardians who believe there has been a possible breach of student data should direct their concerns/complaints to the District Data Protection Officer, Kirsten DeMento at 518-629-3231 or kdemento@vlietschools.org.

6) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Watervliet City School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

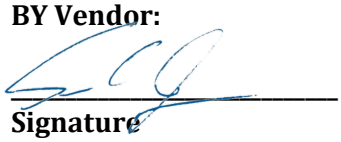
1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.
7. Third-party contractors are also required to:

    a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student date or teacher or principal data;
    b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
    c. Not use educational records for any other purpose than those explicitly authorized in the contract;
    d. Not disclose personally identifiable information to any other party without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
    e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
    f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law 2-d;
    g. Notify Watervliet City School District of any breach of security resulting in an unauthorized release of student data, in the most expedient way possible and without unreasonable delay;
    h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
    i. Provide a signed copy of this Bill of Rights to the Watervliet City School District thereby acknowledging that they aware of and agree to abide by this Bill of Rights.

8) This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department Chief Privacy Officer, as well as emerging guidance documents.

BY Vendor:



Signature

Director, Security Ops & Compliance

Title

10-17-2024

Date

SUPPLEMENTAL INFORMATION

ABOUT THE AGREEMENT BETWEEN
WATERVLIET CITY SCHOOLS AND Vendor

Watervliet City Schools has entered into An Agreement ("AGREEMENT") with Vendor ("Vendor"), which governs the availability to the district of the following Product(s):

Pursuant to the AGREEMENT, the district may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used:

EduClimber

Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the AGREEMENT and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [*Describe steps the Vendor will take*]

Duration of AGREEMENT and Protected Data Upon Expiration:

- The AGREEMENT commences on July 1, 2024 and expires on June 30, 2027. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors. If requested by the district, the Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At THE DISTRICT request, Vendor will cooperate with THE DISTRICT as necessary in order to transition
  Protected Data to any successor Vendor prior to deletion.
- Vendor agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

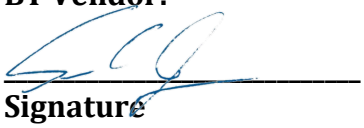
Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the district to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights

and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

BY Vendor:



Signature

Director, Security Ops & Compliance

Title

10-17-2024

Date

Renaissance

See Every Student.

Information Security Overview

Welcome educators! As a leading provider of technology products to K–12 schools worldwide, information security is a critical aspect of Renaissance's business. We abide by our regulatory obligations and strive to exceed the expectations of the educators we serve. Every day, millions of users depend upon our commitment to protect their data. We take this commitment seriously.

This Information Security Overview describes the ways in which we protect your data. If you are interested in learning more about how we handle the privacy of your data (data use, collection, disclosure, and deletion) please visit our Privacy Hub for more information.

Technical Controls

Data Storage & Hosting

Cloud-Hosted Products:

Renaissance cloud products are designed around the core pillars of confidentiality, integrity, and availability. Renaissance products are developed, tested, and deployed in Amazon Web Services (AWS) and Google Cloud Platform (GCP) across several geographically and logically separated locations. AWS and GCP comply with an array of industry recognized standards including ISO 27001 and SOC 2.

Amazon Web Services (AWS) Hosted Products:

Renaissance Growth Platform, Freckle, myON, Schoolzilla, Star Phonics, Lalilo, eduCLIMBER, FastBridge, eSchoolData

For more information about AWS, please visit https://aws.amazon.com/about-aws/global-infrastructure/.

Google Cloud Platform (GCP) Hosted Products:

SchoolCity, DnA, eduCLIMBER

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:

The Renaissance Data Center (RDC) serves our international Renaissance Place customers and is located in Wisconsin, USA. Renaissance Place runs on dedicated servers, network infrastructure, and data stores. Each customer's data is stored in a separate database that operates independently of all other customers' databases. Each school or trust that uses Renaissance Place has its own unique Renaissance hosted site URL, and each user is assigned unique login credentials.

Data Location & Vendors/Sub-Processors

See our list of Sub-Processor information.

Encryption

Data encryption is an important component of the protection of sensitive data. Renaissance's security team consistently reviews, and updates encryption controls based on the latest standards and guidelines published by Open Web Application Security Project (OWASP) and National Institute of Standards and Technology (NIST).

- *In transit:* Renaissance requires encryption over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes.
- *At rest:* Renaissance requires encryption using industry standard Federal Information Processing Standards (FIPS) approved encryption algorithms.

Credentials and Role-Based Access

Each school or district has a unique identifier within Renaissance products. Each user is assigned unique login credentials, which must be authenticated before the user can access the school or district site. Users are assigned to distinct roles, such as student, teacher, or administrator, which limits what information users can access or edit.

Cybersecurity Features

Renaissance implements layered network security controls to protect customers' data. These include Endpoint Detection and Response software and services; next-generation firewalls; segmented design; patching; system hardening processes; and several vulnerability scanning techniques. Renaissance collects and analyzes an array of log data including system logs, system security configuration logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. We monitor systems 24 hours a day, 7 days a week and any suspicious activity is promptly investigated.

Application Security Testing

Dynamic Application Security Testing (DAST) is run against all our applications on a regular basis. The DAST process, which is an integral piece of our software development cycle, tests our software for exploitable weaknesses and vulnerabilities at each stage of the development process.

Penetration Testing

Renaissance engages with a third party to conduct penetration tests on each application and its underlying infrastructure annually. Penetration test results are used to validate all the security controls we've implemented. All penetration test findings are assessed and remediated through our change management processes and product deployment pipelines.

Business Continuity & Disaster Recovery

Renaissance maintains and tests Business Continuity and Disaster Recovery plans to protect your data. Backups are protected using segmentation and vaulting technologies. Additionally, services are deployed into scalable groups and are load balanced across compute and storage services running in geographically diverse availability zones to provide high availability and reduce the risk of service outage. Renaissance also manages much of its cloud infrastructure as code, which facilitates quick recovery or rollback in case of outage, and better transparency into changes in infrastructure over time.

Physical Controls

Cloud-Hosted Products:
Renaissance cloud products are powered by AWS and GCP: durable technology platforms that align to an array of industry-recognized standards. AWS and GCP services and data centers have multiple layers of operational and physical security.

For more information about AWS, please visit https://aws.amazon.com/about-aws/global-infrastructure/.

For more information about GCP, please visit https://cloud.google.com/infrastructure/.

Renaissance Data Center:
The Renaissance Data Center, which hosts the international Renaissance Place product, is located at Renaissance's corporate headquarters in Wisconsin. Entry into Renaissance properties is controlled via employee magnetic key entry.

Only Cloud Operations and Network Services personnel who are responsible for management of data center infrastructure are allowed unescorted access to the Renaissance data center. Admittance to the data center itself is controlled through a proximity card access system and a motion-based detection system. All visitors to the data center, as well as their internal employee escorts, must sign an access log. We also monitor log files, review access logs, track system usage, and monitor network bandwidth consumption.

The environmental conditions within the data center are maintained at a consistent temperature and humidity range, with a third-party security firm monitoring conditions within the data center. Should any changes in power or temperature occur, key Renaissance personnel are notified. Electrical power is filtered and controlled by dual uninterruptible power systems. If a power outage occurs, an automatic-start generator provides uninterrupted power to our servers and heating, ventilation, and air conditioning units. A waterless fire protection system and an early-warning water detection system help to prevent damage to the servers that store our customers' data.

Administrative Controls

Risk Management and Governance

Our security processes and controls substantially follow the FIPS 200 standard and NIST Special Publication 800-53. Renaissance also assesses its Information Security and Privacy programs against the Center for Internet Security (CIS) Top 18 Controls and the NIST Cybersecurity Framework (CSF).

Cybersecurity Risk Committee: The Renaissance Cybersecurity Risk Committee is charged with identifying, tracking, and managing cybersecurity risks. The committee communicates with executive leadership and the board of directors to keep them informed of key cyber and business level risks facing Renaissance. The Committee is also charged with evaluating Renaissance information security and privacy policies, procedures, and operations along with Renaissance's products, product development, and product deployment systems to identify potential areas of vulnerability and risk. These evaluations are used to develop policy, practices, and processes aimed at mitigating or removing vulnerabilities and risks. The Committee assesses all observed and perceived risks to develop policy, practices, and priorities to manage risk to an acceptable level.

Incident Response Team

Renaissance maintains an Incident Response Plan and has a standing Incident Response Team. The Incident Response Team performs Tabletop Exercises at least twice annually. Tabletop Exercise results are used to further refine the Incident Response Plan, policy, and risk management practices.

Renaissance collects and analyzes an array of log data including system logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. Monitoring and analysis of collected data occurs 24 hours a day, 7 days a week and any suspicious activity is promptly investigated and reported to responders.

Renaissance's employees and agents are obligated to protect all customer data. This includes reporting any suspected or known security breaches, theft, unauthorized release, or unauthorized interception of customer data. Should evidence of an information security incident arise, our Incident Response Team will initiate the response plan.

We encourage district representatives with any questions or concerns regarding privacy, security, or related issues to contact our Chief Information Security Officer via e-mail at infosecurity@renaissance.com.

Security Education, Training & Awareness

All Renaissance employees are required to complete Privacy and Information Security training on an annual basis. Renaissance regularly communicates information about the current cybersecurity threat landscape to all employees. Additionally, Renaissance conducts an anti-

phishing and social engineering awareness and training program. Supplemental training events, such as International Privacy Week and Cybersecurity Awareness Month, are also major elements of the training program.

Compliance

Audits: Renaissance's enterprise Information Security & Compliance Program successfully completed the SOC 2 Type 1 examination of controls in November 2022. The examination is formally known as a Type 1 Independent Service Auditor's Report on Controls Relevant to Security, and reports on Renaissance's systems and the suitability of the design of our controls. Our SOC 2 Type 1 is scoped to specific products and services. For more information on our SOC audits, including which products have completed SOC audits, please contact infosecurity@renaissance.com.

Renaissance's enterprise Information Security & Compliance Program intends to complete a SOC 2 Type 2 examination of controls in 2023 and annually thereafter.

Employees: All Renaissance employees must sign a nondisclosure agreement prior to the start of their employment. Additionally, all employees are required to read, sign, and agree to abide by Renaissance's Information Security and Information Technology policies. Background checks are conducted as part of the onboarding process for employees to the extent permitted by law.

Vendors/Sub-processors that Support Our Products: Renaissance maintains a vendor compliance program. Vendors' security and privacy practices are reviewed and analyzed. Additionally, Renaissance enters into written contracts with each vendor/sub-processor containing terms that offer similar levels of data protection obligations and protection for customer personally identifiable information as identified in our Data Protection Addendum with customers.

If you have specific information security questions, please contact:
infosecurity@renaissance.com