Dun & Bradstreet Inc.
System and Organization Controls (SOC) 3 Report
Report on the Data Cloud Products and Solutions System Relevant to Security, Availability, and Confidentiality
For the period February 1, 2019 to July 31, 2019
Report of Independent Accountants

To the Management of the Dun & Bradstreet Inc.

Approach

We have examined management’s assertion that Dun & Bradstreet Inc. (D&B) maintained effective controls to provide reasonable assurance that:

- The Administration of the Data Cloud Products and Solutions System was protected against unauthorized access, use, or modification to achieve D&B’s commitments and system requirements
- The Administration of the Data Cloud Products and Solutions System was available for operation and use to achieve D&B’s commitments and system requirements
- The Administration of the Data Cloud Products and Solutions System processing is complete, valid, accurate, timely, and authorized to achieve D&B’s commitments and system requirements
- The Administration of the Data Cloud Products and Solutions System information is collected, used, disclosed, and retained to achieve D&B’s commitments and system requirements

during the period February 1, 2019 to July 31, 2019 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants’ TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria). This assertion is the responsibility of D&B’s management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of D&B’s relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating D&B’s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.
Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, D&B’s management’s assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Ernst & Young LLP

November 5, 2019
Boston, Massachusetts
Management’s Assertion Regarding the Effectiveness of Its Controls
Over the Data Cloud Products and Solutions System
Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

November 5, 2019

We, as management of Dun & Bradstreet Inc. (D&B), are responsible for designing, implementing and maintaining effective controls over the administration of the Data Cloud Products and Solutions (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity’s Security’s controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period February 1, 2019 to July 31, 2019 to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, and confidentiality (Control Criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria). Based on this evaluation, we assert that the controls were effective throughout the period February 1, 2019 to July 31, 2019 to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification to achieve D&B’s commitments and system requirements
- The System was available for operation and use, to achieve D&B’s commitments and system requirements based on the Control Criteria.
- The System processing was complete, valid, accurate, timely, and authorized to achieve D&B’s commitments and system requirements
- The System information was collected, used, disclosed, and retained to achieve D&B’s commitments and system requirements based on the Control Criteria.

Our attached description of the boundaries of the Data Cloud Products and Solutions system identifies the aspects of the system covered by our assertion.

Dun & Bradstreet
Description of Dun & Bradstreet’s Data Cloud Products and Solutions relevant to Security, Availability, and Confidentiality

Overview of D&B’s Data Cloud Products and Solutions

Corporate Overview

D&B transforms commercial data into valuable insight which is the foundation of our global solutions that customers rely on to make critical business decisions.

D&B provides solution sets that meet a diverse set of customers’ needs globally. Customers use Risk Management Solutions™ to mitigate credit, compliance and supplier risk, increase cash flow and drive increased profitability. Our Sales & Marketing Solutions™ help customers better use data to grow sales, digitally engage with customers and prospects, improve marketing effectiveness and allow for data management capabilities that provide effective and cost-efficient marketing solutions to increase revenue from new and existing customers.

D&B Data Products Descriptions

<table>
<thead>
<tr>
<th>D&amp;B’s Data Cloud Products and Solutions</th>
<th>Product Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D&amp;B Hoovers</td>
<td>D&amp;B Hoovers delivers a sales acceleration platform packed with insight, so customers can target more strategically, have better informed conversations, and enhance the productivity of their sales and marketing teams. The product helps accelerate sales with more leads, improved win-rates, and shortened sales cycles.</td>
</tr>
<tr>
<td>D&amp;B DataVision</td>
<td>D&amp;B DataVision leverages business records from several sources across various geographies to help marketer’s profile, visualize, and segment data to identify the right targets for growth.</td>
</tr>
<tr>
<td>Data Integration Batch</td>
<td>Data Integration Batch consists of cleanse/match/append processing for customers and delivery of prospect universe files. Customers need DUNS Numbers on their records to take advantage of D&amp;B risk, marketing, or supply data, all enabled through batch flat-file processing, matching, and data append.</td>
</tr>
<tr>
<td>DNBi Risk Management (Formerly DNB Interactive - DNB Premium)</td>
<td>DNBi Risk Management is a Software as a Service (SaaS) risk management product suite serving commercial customers. It provides real-time access to D&amp;B data and predictive analysis on global commercial entities to help evaluate financial risk on new customers, and to identify and manage risk and opportunity across a customer’s entire portfolio. DNBi Risk Management has multiple editions based on geography (US, Canada, EU, Australia) and customer segments (Premium, Enterprise), with varying access to modules (Account Manager, Portfolio Risk Manager, etc.) that serve advanced use cases.</td>
</tr>
<tr>
<td>Market Insight</td>
<td>Market Insight is a hosted application that helps enable marketing professionals to apply advanced analytical tools to customer, D&amp;B, and third-party industry data to identify attractive markets, prospects, and up-sell/cross-sell opportunities.</td>
</tr>
<tr>
<td>Small Business Risk Insight</td>
<td>Small Business Risk Insight (SBRI) originated at the request of financial services customers (banks, credit card issuers, etc.) who needed better insight to inform their small business lending decision processes. SBRI is a data repository of commercial credit card, line, loan, and lease financial</td>
</tr>
<tr>
<td>D&amp;B’s Data Cloud Products and Solutions</td>
<td>Product Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>D&amp;B Compliance Check</strong></td>
<td>D&amp;B Compliance Check is a powerful compliance &quot;Know Your Vendor&quot; solution which provides advanced screening, monitoring of third parties and facilitates compliance with global anti-bribery and corruption regulations. It allows global organizations to identify banned, suspect or higher-risk entities, strengthen fraud protection, help ensure regulatory compliance, manage supply and distribution risk, and protect brand equity. It is supplemented by adverse media information from Regulatory Data Corporation's database of global watch lists, regulatory authority actions, law enforcement sources, global news sources and proprietary research, recognized as one of the most robust sources of data available.</td>
</tr>
<tr>
<td><strong>Registration Portal</strong></td>
<td>D&amp;B's Registration Portal capability provides our clients with the ability to automate the third-party data collection process as part of their Third-Party Due Diligence program. Registration Portal is an add-on product within D&amp;B Compliance Check.</td>
</tr>
<tr>
<td><strong>D&amp;B Credit</strong></td>
<td>D&amp;B Credit is a cloud-based risk solution that is globally deployable and meets customer trade-credit requirements through modern interfaces and user experience. Search &amp; find capability includes more intelligence to quickly deliver the right business. The credit reports tell a risk story that enable better credit decisions. Enhanced alert capabilities inform users of any recent risks or opportunities with intuitive navigation and additional supporting data.</td>
</tr>
<tr>
<td><strong>D&amp;B Direct+</strong></td>
<td>D&amp;B Direct+ is a cloud-based API designed to help customers solve various use cases, including Master Data-as-a-Service, Fast Type-Ahead for Custom Lead Forms, Custom Marketing Automation, High Volume Advanced Monitoring, Fast Match &amp; Append, and Custom CRM Integration, among others.</td>
</tr>
</tbody>
</table>
D&B Data Services Descriptions

<table>
<thead>
<tr>
<th>D&amp;B's Data Cloud Products and Solutions</th>
<th>Product Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D&amp;B Match</strong></td>
<td>D&amp;B Match provides services for enriching client’s database with D&amp;B data. Matching is the D&amp;B proprietary process (DUNSRIGHT™) by which an input record (from the customer) is compared to D&amp;B’s company database. D&amp;B will collect, aggregate, edit, and verify data from thousands of sources daily so that customers can use the information to make profitable decisions for their businesses.</td>
</tr>
<tr>
<td><strong>Customer File Processing</strong></td>
<td>Customer File Processing (CFP) is the batch processing system that receives files directly from customers to fulfil records related to the business (i.e., company name, full address, phone number, website domain, c-level/owner contact). The fulfillment process includes cleanse, match, and append process. CFP application also supports appending of data elements for DUNS numbered files. CFP utilizes the SAS data warehouse to append elements for the DUNS provided. CFP applications support appends from mainframe source files through the customized plug and play jobs written specific to each customer requirements.</td>
</tr>
<tr>
<td><strong>Safe Transport</strong></td>
<td>Safe Transport (STP) is used for all internal and external file transfers within D&amp;B.</td>
</tr>
</tbody>
</table>
D&B Architecture Overview

Amazon Web Services (AWS)

AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS provides hosting and resizable computing capacity in the cloud for:

- D&B Credit
- D&B Direct+
- Registration Portal

In turn, D&B assumes responsibility and management of the following:

- Patching and updating Operating systems (Linux, Windows, MySQL)
- Configuration of the AWS-provided security group firewall
- Maintenance and implementation of Information Security policies within the organization and supporting IT environment
- Administering and controlling access to accounts and credentials
- Enabling applicable encryption connections for all interactions with AWS
- Responsible for VPC specific network security requirements and managing rules and access controls lists to secure our S3 buckets
- Ensuring our AWS resources have the appropriate levels of redundancy and isolation

The control process areas applicable to D&B’s customers that are not covered in the scope of this report and are the responsibility of AWS include:

- Data center hosting and cloud services
- Environmental safeguards
- Physical access to hosted systems and resources
- Monitoring system availability

Ensono Data Center Hosting Services

Ensono provides co-location physical hosting services for the following D&B Data Cloud Products and Solutions:

- Data Integration Batch
- D&B Match
- Customer File Processing
- Safe Transport
- DNBi Risk Management (Formerly DNB Interactive - DNB Premium)
- Market Insight
- Small Business Risk Insight
- D&B Compliance Check

D&B relies on Ensono to perform data center hosting, environmental safeguards, and physical access to hosted systems and resources. Data center processes and controls are managed and delivered to D&B by Ensono and are not included in the scope of this report.
In turn, D&B assumes responsibility and management of the following:

- Specifying users’ access rights into their applications and databases, including the mainframe; client/server applications; and Oracle, SQL, and similar databases.
- Communicating to Ensono a current list of user entity employees who have security administrative and/or security approval authority. Changes are also communicated to Ensono as needed.
- Communicating to Ensono the security access levels that should be assigned to Ensono support personnel who help resolve security or operational issues.
- Ensuring controls are in place for managing a current list of users who are allowed access to a user entity emergency or ‘Firecall’ IDs if any exist.
- Patching and updating Operating systems (Linux, Windows, MySQL)
- Configuration and implementation of firewalls and rules.
- Maintenance and implementation of Information Security policies within the organization and supporting IT environment.
- Enabling applicable encryption connections.
- Establishing for network security requirements and managing rules and access controls lists.
- Ensuring our resources have the appropriate levels of redundancy and isolation.

The control process areas applicable to D&B’s customers that are not covered in the scope of this report and are the responsibility of Ensono include:

- Data center hosting
- Environmental safeguards
- Physical access to hosted systems and resources

**INAP Data Center Hosting Services**

Dun & Bradstreet utilizes INAP in Somerville, MA for co-location physical hosting services for the following:

- D&B Hoovers
- D&B Datavision

D&B relies on INAP to perform data center hosting, environmental safeguards, and physical access to hosted systems and resources. Data center processes and controls are managed and delivered to D&B by INAP and are not included in the scope of this report.
In turn, D&B assumes responsibility and management of the following:

- Applying logical access security controls, including user authentication, password complexity requirements, password history requirements, password change procedures, account lockout procedures, and related procedures
- Protecting and maintaining the network security of system resources (for example, secure VPN, configuration and use of firewalls and intrusion detection, and disabling of unneeded network services
- Maintaining system components and configurations, including the application of change controls and procedures as necessary
- Maintaining Data encryption controls and the secure transfer of data through networks, including public, semi-private, and virtual private networks
- Performing data backup procedures and data classification procedures as necessary
- Protecting systems against infection by computer viruses, malicious codes, and unauthorized software

The control process areas applicable to D&B’s customers that are not covered in the scope of this report and are the responsibility of INAP include:

- Data center hosting
- Environmental safeguards
- Physical access to hosted systems and resources