



# ENVESTNET

## **SOC 2 REPORT**

FOR THE

UNIFIED MANAGER PLATFORM

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S  
REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY,  
PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY

OCTOBER 1, 2021, TO SEPTEMBER 30, 2022

Attestation and Compliance Services



**Proprietary & Confidential**

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Envestnet, Inc., user entities of Envestnet, Inc.'s services, and other parties who have sufficient knowledge and understanding of Envestnet, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

# TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT .....	1
SECTION 2	MANAGEMENT'S ASSERTION .....	5
SECTION 3	DESCRIPTION OF THE SYSTEM .....	7
SECTION 4	TESTING MATRICES .....	32
SECTION 5	OTHER INFORMATION PROVIDED BY ENVESTNET.....	69

# **SECTION I**

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Envestnet, Inc.:

### Scope

We have examined Envestnet, Inc.'s ("Envestnet" or the "service organization") accompanying description of its Unified Manager Platform (UMP) system, in Section 3, throughout the period October 1, 2021, to September 30, 2022, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Envestnet's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Envestnet uses a subservice organization for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Envestnet, to achieve Envestnet's service commitments and system requirements based on the applicable trust services criteria. The description presents Envestnet's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Envestnet's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Envestnet" is presented by Envestnet management to provide additional information and is not a part of the description. Information about Envestnet's management's responses to exceptions noted and additional information provided by management has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Envestnet's service commitments and system requirements based on the applicable trust services criteria.

### Service Organization's Responsibilities

Envestnet is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Envestnet's service commitments and system requirements were achieved. Envestnet has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Envestnet is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

#### *Inherent Limitations*

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is 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.

#### *Description of Test of Controls*

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

#### *Opinion*

In our opinion, in all material respects:

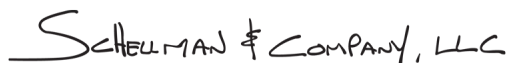
- a. the description presents Envestnet's UMP system that was designed and implemented throughout the period October 1, 2021, to September 30, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Envestnet's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Envestnet's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Envestnet's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Envestnet's controls operated effectively throughout that period.

### *Restricted Use*

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Envestnet, user entities of Envestnet's UMP system during some or all of the period October 1, 2021, to September 30, 2022, business partners of Envestnet subject to risks arising from interactions with the UMP system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

SCHELMAN & COMPANY, LLC

Chicago, Illinois  
November 11, 2022

## **SECTION 2**

### **MANAGEMENT'S ASSERTION**



## MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Envestnet's UMP system, in Section 3, throughout the period October 1, 2021, to September 30, 2022, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the UMP system that may be useful when assessing the risks arising from interactions with Envestnet's system, particularly information about system controls that Envestnet has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Envestnet uses a subservice organization for data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Envestnet, to achieve Envestnet's service commitments and system requirements based on the applicable trust services criteria. The description presents Envestnet's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Envestnet's controls. The description does not disclose the actual controls at the subservice organization.

We confirm, to the best of our knowledge and belief, that:

- a. the description presents Envestnet's UMP system that was designed and implemented throughout the period October 1, 2021, to September 30, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Envestnet's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of Envestnet's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout the period October 1, 2021, to September 30, 2022, to provide reasonable assurance that Envestnet's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Envestnet's controls operated effectively throughout that period.

## **SECTION 3**

### **DESCRIPTION OF THE SYSTEM**

---

## OVERVIEW OF OPERATIONS

### Company Background

Envestnet, Inc. (Envestnet), a publicly traded company (NYSE: ENV), was founded in 1999 to provide financial services to the investment and wealth management sectors and is headquartered in Berwyn, Pennsylvania.

Currently, Envestnet provides services to clients throughout the United States. In addition to the corporate headquarters, Envestnet has offices in Denver, Colorado; San Mateo, California; Raleigh, North Carolina; and Trivandrum, India.

### Description of Services Provided

Envestnet provides services to help clients, including financial institutions and independent advisors, deliver solutions to their clients via Web-based platforms. The Web-based platforms provide access to multiple investment programs, proposal generation tools, and account management resources to help develop and grow advisors' fee-based business. Envestnet provides the Advisory platform (Unified Manager Platform or "UMP") to support clients.

For the purposes of this report, the below key terms are defined:

- Client (user entity) – a customer of Envestnet that purchases the UMP services for use by their employees. This term includes financial institutions and independent advisors.
- Advisor – an employee of a client who uses the platform for daily investment activities.
- Investor – a customer of a client who receives investment advice, reporting, and management from the client.
- Channel – a channel is a group of web servers and databases servers that house and process data for a specified group of clients. Clients are bifurcated into channels in order to ensure consistent UMP data processing efficiency.

### Envestnet Overview

The primary goal of Envestnet is to advise, invest, report, and manage investors' money. The platform is designed to simplify the way advisors manage investor portfolios allowing advisors to research available investments, generate proposals, enter service requests, review investor billing, obtain performance reports, etc. The platform is used by advisors, clients, and Envestnet support teams. Due to the relationships and hierarchy between these groups, the platform takes on different roles and views depending on the user. The platform does not solely benefit one type of user because its capabilities meet the needs ranging from small private firms or investors to large institutions.

The platform gives advisors the resources and ability to research, filter, compare, and model investment products that adhere to the needs and risk tolerances of investors. The platform can be implemented on a stand-alone basis or integrated easily with existing proprietary products, custodial partnerships, and other relationships. Furthermore, the platform can be customized to include features and functions that reflect the client's branding or desired image in the marketplace.

### Services Provided by Envestnet

The scope of this report includes the services and related controls related to processing on the Envestnet platform. Envestnet provides the following services:

#### *Investment Programs – Programs Facilitated by UMP*

- Separately Managed Account Solutions (MAS) – The MAS provides investors with access to some of the leading investment managers. With a separately managed account, investors can enjoy direct ownership of the securities in the portfolio. This may allow for greater flexibility, more control, and significant tax advantages over other investment vehicles.

- Mutual Fund Solutions – The mutual fund solutions provide investors with access to some of the leading mutual funds available.
- Exchange Traded Funds (ETFs) – The ETFs provide investors with access to some of the leading exchange traded funds available.
- Alternate Investments – Access and comprehensive program support of Envestnet's alternate investment product program. Manager research, account administration, and account reporting services for the alternate investment products will differ from those provided for other products offered and will likely differ among the various alternate investment products themselves.
- Reporting Program – Envestnet offers a separate reporting program which consists of online performance reporting for investor accounts that are not part of the above-mentioned programs. The platform reporting capabilities include online, ad-hoc, and comprehensive performance reporting. Additional capabilities of the platform are:
  - Quarterly performance reports posted online by the 20th business day following quarter end.
  - Dynamically created .pdf quarterly performance reports in private-labeled format.
  - Goals-based reporting and monitoring.
  - Custom account grouping.
  - Dashboard reporting for consolidated views at the client level.

#### *Research – Facilitated by UMP*

- Manager Research, Performance Analysis, and Due Diligence:
  - In-depth manager research reports, including summaries and expanded reports, suitable for client/advisor distribution to investors.
  - Quarterly asset manager and fund performance reporting and analysis.
  - Selection, due diligence, and oversight of the investment program.
  - Asset manager commentaries and market outlooks.
  - Online search and screening tools.
  - Asset manager and product access.
- Sigma Portfolio Management Consulting (PMC) Mutual Fund Solution Program:
  - The *Sigma PMC Mutual Fund Solution* offers investors an actively managed portfolio comprised of carefully selected mutual funds.
  - The *PMC Select Mutual Fund Wrap and Portfolios* offers investors an actively managed portfolio comprised predominately of the PMC funds. Envestnet selects the institutional mutual fund managers to participate in this wrap program.

#### *Retirement Solutions*

- Envestnet Retirement Solutions provides a retirement practice suite of solutions that include:
  - Compliance Advantage – Provides plan information, tools, and solutions to help retirement plan fiduciaries deliver quality information efficiently.
  - Practice Advantage – Provides a practice management dashboard and integrated solution to support an entire retirement practice.
  - Fiduciary Advantage – Provides fiduciary support to plan sponsors and their participants.

#### *Outsourced Back-Office Operations and Portfolio Administration Services*

- Account Administration, Billing, and Reconciliation facilitated by UMP. Envestnet offers the following services to clients:
  - Daily reconciliation of cash and positions between custodian and Envestnet systems.

- Account set-up.
- Asset manager set up and account funding.
- Back office and account administration.
- Program billing, including calculation, remittance, and processing of account fees.

---

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Envestnet (herein also referred to as 'we') designs its processes and procedures related to the UMP system to meet its objectives. Those objectives are based on the service commitments that Envestnet makes to user entities, the laws and regulations that govern the provision of the UMP system, and the financial, operational, and compliance requirements that Envestnet has established for the services. The UMP system is subject to the relevant regulatory and industry information and data security requirements in which Envestnet operates.

Security, availability, processing integrity, confidentiality, and privacy commitments to user entities are documented and communicated in customer agreements, company policies and procedures, and the description of the service offering provided online. The principal security, availability, processing integrity, confidentiality, and privacy commitments are standardized and include, but are not limited to, the following:

### Security

- We provide and maintain a secure environment to process customer data in accordance with industry standard security practices.
- We adhere to applicable laws and regulations regarding the security of any of the customer data.
- We monitor the environments for security breaches or violations.
- We implement policies, processes, and controls to remedy any security breach of which we become aware and will notify affected customers in accordance with legal and regulatory requirements.
- We maintain an information security program that includes appropriate administrative, technical, and physical safeguards reasonably designed.
- We periodically assess the computing environment to identify and remediate issues affecting the operation of internal controls.

### Availability

- We utilize enterprise monitoring systems to continuously monitor network and computer systems.
- We monitor service availability to ensure it is in accordance with defined service level agreement (SLA) requirements.
- We backup systems and customer data according to predefined schedules and provide secure storage of backups for the recovery of customer data in the event of a system failure or other loss.

### Processing Integrity

- We implement appropriate technical and organizational controls to ensure the data integrity and resilience of relevant systems and services.

### Confidentiality

- We retain and/or dispose of data in accordance with contractual requirements.
- We encrypt customer data during transmission and at rest using methods that meet current industry best practices.

## Privacy

- We do not sell consumer personal information about a current or former account to third parties.
- We comply with financial laws and regulations to maintain records for statutorily required periods of time.
- We maintain security measures to safeguard against loss, theft, interference, and misuse, as well as unauthorized access, disclosure, alteration, or destruction of personal information.
- Should we make a material change to the Privacy Policy, we will post those changes on the company website with an updated effective date.

Envestnet establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the UMP system.

In accordance with the assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

---

## COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

### **System Boundaries**

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

### **Infrastructure and Software**

The UMP system is developed and maintained by Envestnet. The UMP system has its own process and dedicated support team to provide development and production support.

The UMP system was developed using Java and structured query language (SQL) languages. The platform is highly configurable which makes it flexible for both clients and information technology (IT) support teams. The platform is offered to clients as software-as-a-service (SaaS) via the Internet.

The UMP system runs entirely on Microsoft Windows operating systems (OS). The UMP system is a logical three-tier design, in a physical two-tier implementation including a demilitarized zone (DMZ) and private network. The business logic exists in the middle tier as a Java-based application, with Internet Information Services (IIS) serving web pages in the DMZ and SQL Server on a private network segment. There is a firewall between the database and web/application servers. The production environment is virtualized with no dedicated hardware or resources provided by or for a client. Additionally, clients may be grouped into channels containing specific Envestnet web servers and database servers, but all clients are provided access to the same version of the UMP system.

The network and infrastructure supporting the platform is secured by software and hardware tools, which include but are not limited to perimeter firewalls, antivirus and spyware software, encryption, and security monitoring. Secure data transfer protocols are used to protect data processed by the platform. Client files are encrypted during backup and transmission. Envestnet uses hypertext transfer protocol secure (HTTPS), extensible markup language (XML), secure file transfer protocol (SFTP), etc. as the primary integration methods. In addition to the primary

integration methods, client data is protected with firewalls, network segmentation, and limited-access security permissions. Envestnet leverages Microsoft's transparent data encryption (TDE) to encrypt Microsoft SQL databases when in an offline state. Additionally, TDE provides encryption for the Microsoft SQL database backup files.

Envestnet offers multiple levels of configuration within the platform that can be set at the Advisor level or by hierarchy. The various levels in the hierarchy are enterprise, firm, branch, advisor, and client. The platform offers Advisors different levels of access through role-based entitlements, which are made available to them through configuration settings. An entitlement can enable an advisor to make decisions or view activities at their level and other levels downstream. The platform has an advisor console where advisors are granted access. Based on agreement between clients/advisors and Envestnet, the clients/advisors may determine the roles and permissions assigned to their investors in order to administer their setup configurations within UMP.

Envestnet's primary and secondary data centers are collocated with Cyxtera Data Centers, Inc. (Cyxtera) in Chicago, Illinois, and Highlands Ranch, Colorado, respectively. Cyxtera provides internet bandwidth and colocation services and therefore has primary responsibility for the physical and environmental controls supporting the platform. Envestnet manages logical access controls for the Envestnet owned and operated equipment (servers, storage, firewalls, and network devices) collocated at Cyxtera. Physical security controls and the services provided by Cyxtera are not included within the scope of this report.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
UMP	Platform used to advise, invest, report, and manage Investors' money.	Windows	Chicago, Illinois
Active Directory	Used to manage user accounts, application access, and authentication requirements.		
Servers	Used for virtual application delivery.		
Databases	Used to store, retrieve, and manage data input into the system.	SQL Server	
Firewalls	Used to protect the network perimeter and limit inbound and outbound access.	Palo Alto / Check Point	

People

Work is distributed across Envestnet offices with technology, operations, sales, and support functions in each location, although specific offices are sources of specialized capabilities (e.g., account balancing, system development). Duties are segregated between Envestnet and its user entities. User entities do not perform IT operations, application development or maintenance, systems maintenance, or other Envestnet functions. The organization of Envestnet provides for segregation of duties between account operations, technology, system development, platform support, and user entity support services. Envestnet personnel do not act in the capacity of, or have responsibilities as, an officer, director, or associate of a user entity.

The Envestnet organization is categorized into the following functional areas:

- Executive Management – Executive management is charged with the strategic direction and oversight of operations. They set sales, operational, technical, and financial policies, and review processes to determine whether compliance standards are met.
- Sales and Advisory Services – The sales and advisory services team consists of regional sales representatives and a client services group. This team brings advisors understanding of additional wealth management investment options and support in the day-to-day management of the advisor's practice.



- **PMC** – PMC provides research on managers, markets, and topical issues; and works with Advisors to develop portfolio solutions tailored to the unique circumstances of their investors. PMC helps identify solutions for investor needs and objectives, assists in determining asset allocation policy, recommends asset managers, and provides asset manager due diligence and monitoring.
- **Client Billing** – The client billing team is located in the Denver office and is responsible for a wide range of tasks as they relate to billing for UMP clients. The billing team facilitates the following unique billing requirements of clients: fee schedule setup (firm, account, and product level), fee calculation, fee processing, and invoicing.
- **Envestnet Retirement Solutions (ERS)** – ERS provides a retirement practice suite of solutions that include compliance advantage, practice advantage, and fiduciary advantage. The ERS team is located in San Mateo, California, and Trivandrum, India.
- **Administration** – The human resources (HR) and facilities department (collectively known as “HR”) is responsible for the recruitment of new employees, employee benefits/compensation, and other employee relations that include the recognition program. HR performs criminal, educational, and financial background checks on candidates. The compliance department is responsible for firm-wide compliance oversight and for the development and implementation of an audit and monitoring program to ascertain compliance with applicable laws/regulations. In addition, the compliance department aids in the development of policies and procedures to prevent and detect unlawful activity. Envestnet employees are required to attend training to become familiar with the culture of compliance. The accounting/finance department consists of purchasing, accounting, reconciliation, and budget analysis activities.
- **Technical Support** – The technology services (tech services) teams in Raleigh, North Carolina, Berwyn, Pennsylvania, and Trivandrum, India, are responsible for the day-to-day operational support of the platform, and coordination with the support teams in Trivandrum to ensure the platform adheres to the service level agreements that have been agreed upon with the clients. The information security team sits in Trivandrum, India, and is responsible for the facilitation of production infrastructure user access reviews. The site reliability engineering (SRE) team is responsible for the maintenance of the systems, including database servers, web servers, application servers, utility servers, networking and technical infrastructure components, and information security. The help desk resides within SRE and is responsible for access provisioning/de-provisioning for corporate resources and the production domains. Development teams are responsible for requirements, design, code and unit testing for releases, enhancements, and bug fixes. Overall direction of UMP development activity is provided by the UMP engineering and product management organization, which is divided into four sub-teams to facilitate prioritization and delivery of enhancements. Quality assurance (QA) is responsible for testing changes prior to deployment, as well as verifying changes post deployment. The release team, located in San Mateo, California, and Trivandrum, India, is responsible for building releases from the code repository for production deployment.
- **Operations** – Portfolio accounting services (PAS) provides support for a variety of teams within Envestnet. They are responsible for daily account reconciliations and addressing client requests and issues prior to trading opening on the UMP system. The team also provides client support for the MAS team. The MAS team, located in Berwyn, Pennsylvania, and Trivandrum, India, serves as the back-office operational support for Envestnet broker/dealer and registered investment advisor (RIA) service models. The team is split into several sub-teams: broker/dealer (B/D) model, RIA model, and digital advice. The MAS team works to provide support internally to client facing departments such as institutional client services (ICS) and customer service group (CSG), and also works closely with other operations teams to ensure accurate and timely back-office processing for the investors.
  - The B/D model team is responsible for open registrations, changes to the statement of investment selection, dollar cost average process, bond sleeve monitoring for affected accounts regardless of service model, and investment manager interactions.
  - The RIA model team is responsible for custodian interactions, money movement, and account maintenance and issue resolution.
  - The digital advice team is responsible for open registrations, “not in good order” (NIGO) communications to investors, money movement, transfer of assets, account maintenance, and B/D and RIA firm interactions.



## **Procedures**

### *Access Authentication and Authorization*

Envestnet maintains information security policies that include information on security roles and responsibilities of various levels of management, Internet security, computer and network security, use of corporate services, Internet/intranet usage, and consequences of security violations.

Envestnet uses a multi-layered approach to protecting resources and assets. This includes physical security and logical security from desktop through the network and server environments. Access to system information, including confidential data, is protected by authentication and authorization mechanisms. The in-scope systems are configured to authenticate users with a unique user or designated administrator account and enforce predefined user account and minimum password requirements including minimum password history, password expiration intervals, minimum password length, password complexity, and an invalid password account lockout threshold. Access to production systems varies by system and is ultimately restricted via Active Directory permissions (applicable to domain controllers, servers, databases, application, and firewall). Encrypted virtual private networks (VPNs) are utilized for remote access for the security and integrity of the data passing over the public network.

Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems. Administrative access privileges are initiated and approved by the employee's manager using a security access form, restricted to authorized personnel, and are responsible for assigning and maintaining access rights to the production environment.

### *Access Requests and Access Revocation*

A defined user access management process is in place. HR initiates the new employee access provisioning process by submitting an access request to the help desk. IT personnel are responsible for assigning and maintaining access rights to the production environment and follow a documented process to add, modify, or remove access for employees. Employees are assigned a unique network domain account, and access requests are documented within the ticketing system and require manager approval. Access is subsequently granted based on the employment position. The UMP production environment is separate from the corporate network domain. Employees who require access to the production environment are authorized and assigned a separate distinct production user account to that environment. Production domain users are given accounts that expire annually to ensure their privileges are reviewed periodically.

Upon notification from HR of an employee termination, a termination ticket is created and system access is revoked by sending the termination information to the access change distribution list. Depending on the sensitivity and/or urgency, the initial termination notice given to IT may be verbal. The access change distribution list contains a list of platform, network, and infrastructure stakeholders that have security administration responsibilities for the enterprise or a business area. The stakeholders confirm via e-mail that the terminated employee's access has been revoked.

IT personnel perform a review of privileged access privileges including the UMP production domain, web application servers, and database servers on a quarterly basis to verify that administrative access privileges are assigned to authorized personnel and that system access levels are commensurate with current job responsibilities. When a user is identified who no longer requires access to the systems, their access is subsequently revoked. Additionally, IT personnel perform a user access review of UMP personnel annually. Managers confirm the entitlements of their direct reports. Access that is not confirmed or identified as no longer needed is removed as a result of the process.

### *Systems and Networking Change Management*

The SRE team follows a change management procedure to ensure quality and consistency when making network or infrastructure changes. The SRE team submits change requests via the change management system to document the change request and updates the change request when it is complete. Types of changes include UMP package deployments, software updates, server updates, security patches, etc. Change requests are reviewed and approved.

### *Platform Development and Maintenance*

There is a development and support team for UMP, with their own systems development lifecycle and tools used to facilitate tri-annual releases for UMP, patches, and production support. There are scheduled releases as well as

patches and enhancements that may be implemented in between releases. The platform team uses a source code management tool and issue/change tracking tool to facilitate the change management process. The change management process is designed to enforce segregation of duties throughout the end-to-end process, based on the roles and responsibilities assigned to the development, release, and SRE team.

UMP development and maintenance is performed by the Envestnet development staff in Raleigh, Berwyn, and Trivandrum. Changes to the development policies and procedures are made under the authority of the UMP engineering team and product management directors.

The defined roles for personnel involved in the UMP platform definitions (development, verification, and implementation) are as follows:

- Code developers: members of the development team responsible for the programming tasks.
- Database (DB) change coordinator: the member of the UMP development management team who is responsible for the review and distribution of database changes done by UMP development management team members.
- Release note coordinator: responsible for the review and final documentation of the UMP release notes.
- QA team/independent verification & validation (IVV) team: verification of software releases is performed using a documented test plan developed from the functional specification document (FSD) by the QA team independent of development. The QA testing is done in a QA environment simulating the production environment. The new enhancements are tested by smaller teams of testers within each pod referred to as pod QA. The QA team who performs the focused regression testing is referred to as IVV. The IVV team works closely with the pod QA in assessing the complexity of the change. The QA testing includes the testing of the fixes released through the weekly patches as well as the regression testing of the affected modules. QA certification of the release is required before the release deployment.
- Release team: responsible for building the releases using approved versions from the version control software as requested by development and QA.
- SRE: responsible for maintaining the production environments and deployment of UMP changes based on a help desk request from the release team.
- Development management: responsible for code reviews, process oversight, and signoffs. The team members include the chief technology officer (CTO), director of software development, and manager of software development.

#### UMP Change Management Process

Changes initiated by the business are tracked in the project list within the UMP Platform. Development can also initiate changes to the platform. Changes deployed to production are included in the change request to the help desk, which is stored in the Samanage help desk tool.

The development, QA, and IVV teams in Trivandrum design, code, and QA test changes to the platform. The source code and database scripts are managed using the GitLab tool and must conform to standards before development is concluded.

User acceptance testing (UAT) is done prior to the deployment of changes to production. As part of UAT, business users test the new system functionality to be included in system changes. This involves running business processing scenarios in the test environment.

The IVV team performs regression and new feature testing based on a test plan. The results of the QA test plan are summarized by the QA team manager and sent to development management, who reviews the completed test plan and signs off on the results. For deployment to production, development and SRE coordinate deployment using an agreed upon install strategy. Using scripts, the release team builds a new version of the code from the source code management tool. The build is done under the direction of the director of software development. The new version of the software is deployed to the production environment by SRE. The back out plan for a deployment is to re-deploy the previous version of the software.

Segregation of duties is enforced throughout the process based on the person's role within the change management process (developer, DBA, QA/IVV, release team, SRE) with access privileges that support their role and tools used to facilitate the process.

### *Data Backup*

An automated backup system is utilized to perform scheduled backups of production systems and data at predefined times. The automated backup system is configured to notify IT personnel via e-mail regarding the failure of backup jobs. A restoration of backups is performed as a component of business operations. Envestnet utilizes two separate data centers collocated with Cyxtera to host the production and disaster recovery environments in Chicago, IL and Highlands Ranch, CO, respectively. The data centers provide environmental security and internet bandwidth at the site. Database backups are written directly to disk in the primary data center. In a fail-over scenario, the production virtual machines take over the role of production at the disaster recovery site.

### *Business Continuity and Disaster Recovery*

An enterprise business continuity plan (BCP) is in place to address the framework in which a business disruption would be managed to minimize the loss of vital resources throughout the company. The enterprise BCP in its entirety provides instructions to the business on how to prevent, prepare, respond, and perform tasks with the purpose of developing and providing business resilience in the face of any risk to the continuation of business operations. Envestnet business continuity planning focuses on potential disruptions of key business resources: technology, workspace, and employees. In order to recover quickly the business has established a disaster recovery warm site for critical technology and data. Operational failover sites and employee alternatives are also in place for critical business processes throughout the company.

The enterprise BCP encompasses multiple levels of plans according to the level of responsibility in the business and the actions required. The enterprise BCP provides an overview of plans and procedures for Envestnet stakeholders for use before and during a disruption. Envestnet maintains the following documentation for its business continuity, disaster recovery, and pandemic planning programs:

- Enterprise BCP – The enterprise-level document detailing the BCP program and policy for achievement of regulatory and contractual compliance and industry best practice.
- Envestnet Summary BCP Disclosure – The public summary of the Envestnet BCP and program details how Envestnet maintains compliance with regulatory requirements. The public summary is provided to clients upon request and is published on the corporate website.
- Location Business Resumption Plans – Location-level recovery plans and procedures to achieve recovery of critical business in line with compliance and within the recovery time objective (RTO). In addition, these plans contain building-specific emergency response plans for use in an incident causing building evacuation or an employee health and safety issue, damage assessment forms, and location-specific vendor contacts.
- Department Business Resumption Plans – Department-level procedures providing critical resources, skills, tasks, and SLAs identified through the business impact analysis (BIA) and updated at least annually; includes employee level procedures to achieve recovery in line with compliance and within the RTO. Also identifies alternative employees within the department or in another geographic location that are able to supplement resumption efforts.
- Employee Unavailability Plan/Pandemic Plan – Provides instruction for planning, response, and resumption of the business due to a pandemic, communicable illness, or other events impacting the availability of Envestnet employees.
- Disaster Recovery Plans – Technology-specific plans and procedures to protect critical business from extended outages and to ensure resumption and recovery of defined critical technology within the RTO.

### *Incident Response*

An incident response policy is in place to address the reporting, classification, and handling of information security incidents. The policy is communicated to employees via the company intranet. The incident management team is comprised of members of executive management responsible for incident resolution and prevention. The information security management committee meets on a quarterly basis to discuss incidents and corrective measures to ensure that incidents are resolved.

When a security event is reported or detected, members of the security incident response team examine and evaluate the event. If the security event is escalated to a security incident, it is manually logged in the security incident tracker which is utilized to document actions taken to contain and resolve the security incident. A root cause analysis is performed for security incidents that includes an impact analysis, resolution, lessons learned, and action items.

*System Monitoring*

A security information and event management (SIEM) application is utilized to monitor system events for anomalies that are indicative of malicious acts, natural disasters, and errors. These security events consist of activities within the network, firewalls, intrusion detection system (IDS), servers, databases, and application. The SIEM application analyzes log results and alerts IT personnel via e-mail in the event that suspicious or unauthorized activities have occurred. Additionally, an enterprise monitoring application is utilized to monitor the capacity levels of the in-scope systems and notify IT personnel via e-mail when predefined thresholds are exceeded on monitored devices. These monitoring events include central processing unit (CPU) utilization, storage capacity, and bandwidth usage. An IDS is utilized to analyze and report network events. Logs are collected from the IDS and the enterprise monitoring application.

Regular security reviews and vulnerability assessments are performed by IT personnel and third-party vendors to identify new vulnerabilities and susceptibilities to new vulnerabilities. Such reviews include weekly external vulnerability scans, weekly internal vulnerability scans, and an annual penetration test.

Antivirus software is configured on registered clients to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software is configured to scan for updates to antivirus definitions, update registered clients, and scan registered clients on a continuous basis.

**Data**

Envestnet classifies data and information assets in terms of legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Data of this category is for distribution to individuals explicitly approved by only the data owner. Unauthorized disclosure or use of this information can result in significant or irreparable consequences to Envestnet (compliance failure, breach of contract, loss of revenue, degradation of competitive advantage), individuals (violates the privacy of individuals includes consumers, employees, and vendors), clients, or partners.	<ul style="list-style-type: none"><li>• Data must be processed by approved systems and approved personnel only</li><li>• Data must be encrypted and stored in approved systems with access restricted to authorized personnel only</li><li>• Data must be retained as per client contract, company defined policy, and applicable laws</li><li>• Magnetic hard drives and universal serial bus (USB) flash drives must be physically discarded or wiped using an approved secure wiping program before being re-deployed, send off-site for maintenance or repair, or discarded</li></ul>	Restricted

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Data of this category is for distribution to approved internal and external stakeholders for explicit business purposes. Unauthorized disclosure of this information can have legal implications as well as significant negative consequences to the competitive position, client confidence, and market perception.	<ul style="list-style-type: none"> <li>Data must be processed by approved systems and approved personnel only</li> <li>Data must be encrypted and stored in approved systems with access restricted to authorized personnel only</li> <li>Data must be retained as per company defined policy and applicable laws</li> <li>Magnetic hard drives and USB flash drives must be physically discarded or wiped using an approved secure wiping program before being re-deployed, send off-site for maintenance or repair, or discarded</li> </ul>	Confidential
Data of this category is not sensitive to disclosure internally and may be shared with customers, partners, and clients under nondisclosure agreements with approval from the data owner.	<ul style="list-style-type: none"> <li>Data must be processed by company personnel only</li> <li>Data must be stored in approved systems</li> </ul>	Internal
Data of this category has been explicitly approved for general release and may be freely disseminated.	<ul style="list-style-type: none"> <li>N/A</li> </ul>	Public

### Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

### Subservice Organizations

The data center hosting services provided by Cyxtera were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Cyxtera, alone or in combination with controls at Envestnet, and the types of controls expected to be implemented at Cyxtera to achieve Envestnet's principal service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by Cyxtera	Applicable Trust Services Criteria
Cyxtera is responsible for implementing controls to restrict physical access to facilities and protected information assets.	CC6.4 PC3
Cyxtera is responsible for implementing controls to protect against environmental vulnerabilities and changing environmental conditions.	A1.2

Envestnet has not delegated any responsibility of the personal information life cycle to Cyxtera.

---

## PRIVACY NOTICE

Within the UMP system, Envestnet provides services to user entities in the capacity of a data processor. Envestnet serves in the function of a processor in cases where it processes personal data only as instructed by user entities (data controllers) in order to fulfill the requirements of an agreement associated to the provisioning of the services.

User entities are responsible for providing their privacy notice to individuals. Envestnet communicates its privacy notice to user entities via the company website. The privacy notice is included below and is inclusive of how the organization addresses privacy from both the data controller and data processor perspectives; however, only areas that the service organization acts as the latter are applicable to this review.

### Envestnet Privacy Policy

Envestnet Asset Management, Inc. and its subsidiaries and affiliates, Envestnet Financial Technologies, Inc., Envestnet Portfolio Solutions, Inc., Envestnet Retirement Solutions, LLC, FDX Advisors, Inc., Folio Dynamics Inc. (doing business as FolioDynamix), MoneyGuide, Inc., QRG Capital Management, Inc., and Tamarac Inc. (collectively “Envestnet”, “we,” “us”, or “our”) understand the value of maintaining privacy when handling financial information. We present this Privacy Policy (the “Privacy Policy”) which discloses our privacy practices to respect the privacy of financial information and the security of consumer personal information.

### Authorization of Use

Either you who are using this website (collectively with any co-client, “you”, or “your”) or your financial advisor, benefit plan sponsor, employer, or association (each, your “Representative”) has input your personal information and, if applicable, your co-client’s personal information, into the Envestnet software, products, websites, and/or services (the “Services”), to service your financial account(s) on your behalf, provide you customized financial planning resources, or generally assist you with your overall financial wellness. By using our Services, you agree to abide by the following terms and conditions for the Services. Your financial advisor, benefit plan sponsor, employer, or association (and, if applicable, the firm with whom they are licensed) shall have access to the Services as you have permissioned them to have in your separate agreements with them. Those parties’ use of your personal information is governed by their respective privacy policy(ies). Please contact your financial advisor if you have questions about their firm’s privacy policy.

### Personal Information We Collect

As part of providing a holistic picture of your financial wellness, Envestnet may collect some or all of the following types of personal information:

- Identifiers like postal address, e-mail address, account name, unique personal identifier, login credentials, or other similar identifiers;
- Customer records like a signature, address, telephone number, passport number, social security number, driver’s license or state identification card number, insurance policy number, employment, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information as applicable as required to utilize insurance- related tools;
- Classification characteristics like age, marital status, and sex;
- Commercial information such as records of personal property, investment assets, account activity (including transactions, balances, positions, and history), anticipated retirement expenses, expected values of future assets such as lumpsum distributions from pensions or inheritances, and other purchasing or consuming



histories or tendencies (for example, if you opt to share this information in order to view and analyze spending habits and work on budget performance);

- Internet or other similar network activity, like online identifier, Internet protocol address, web browser, cookie identifiers, and other identifiers that are automatically assigned to your computer or devices when you access the Internet and information on interactions with our Services, other websites, applications, or advertisements;
- Geolocation data such as physical location or movement of devices, as applicable (for example, if accessing the Services through a voice-activated digital assistant);
- Sensory data, such as customer service requests or questions directed to Envestnet through our websites or via telephone conversations;
- Professional or employment-related information, such as current or past job history and income; and
- Inferences drawn from other personal information, such as any additional profile information reflecting preferences and behavior (for example, a person's risk tolerance related to investment strategies).

Envestnet may receive the categories of personal information described above from you, your Representative(s), integration partners, government entities, and third-party data providers who have the rights to provide us with your information. "Personal information" does not include publicly available information from government records used for the purpose for which the information was made publicly available, publicly available business contact information, or de-identified or aggregated consumer information.

## **How We Use Personal Information**

Envestnet does not sell, rent, or lease consumer personal information we collect. In compliance with federal and state laws, we may use consumer personal information for one or more of the following business purposes:

- To fulfill or meet the reason you or your Representative provided personal information in the first place to us;
- To create, maintain, customize, and secure your account;
- To process requests, purchases, transactions, and payments;
- To prevent transactional fraud;
- To provide support and to respond to inquiries, including to communicate with you;
- To provide measurement, analytics, and other business services;
- To personalize and develop experiences with our Services, including offers through our websites, applications, e-mails, and or text message, and other platforms (with your consent, where required by law);
- To help maintain the safety, security, and integrity of our Services, databases, other technology assets and business lines;
- To notify you about any new functions included in our software or services (with your consent, where required by law);
- For testing, research, analysis, and product development, including to develop and improve our Services;
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Envestnet's assets, whether as a going concern or as part of a bankruptcy, liquidation, or similar proceeding, in which personal information held by Envestnet about users is among the assets transferred;
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations;
- As described to you when collecting your personal information; and
- For the reasons otherwise set forth in this Privacy Policy.

Envestnet may develop, use, distribute, and publish information and statistics derived from aggregate consumer information and the content that you contribute for use on a masked, aggregate basis.

### **Cookies, Pixel Tags/Web Beacons, and Similar Technologies**

We, as well as third parties that provide content, advertising, or other functionality to the Services, may use cookies, pixel tags, local storage, and other technologies (“Technologies”) to collect tracking and identification information. The Technologies are essentially small data files placed on visitor device(s) that allow us to record how visitors use the Services, which site a user comes from, the number of each user’s visits, and how long a user stays on the Services. The Technologies help to improve software function, facilitate site navigation, and personalize your experience of the Services. The use of these Technologies is described in our Cookie Policy.

### **Disclosing Personal Information to Others**

We do not sell consumer personal information about a current or former account to third parties. For financial professionals utilizing our technology platform, however, Envestnet may make available financial professional business contact information, financial professional profile information, and information regarding the use of investment strategies to third-party investment managers and exchange traded funds, mutual funds, and similar investment vehicles.

In compliance with federal and state laws, we may disclose personal information to nonaffiliated businesses for a business purpose. We disclose personal information for a business purpose to the following categories of third parties:

- Envestnet corporate affiliates;
- Companies that perform services for us or on your behalf, including the sub-managers who manage your assets and third-party vendors and service providers that provide services to us for a variety of business purposes, such as billing, payment processing, customer service, e-mail deployment, advertising and marketing, security and performance monitoring, maintaining or servicing accounts, processing or fulfilling orders and transactions, verifying customer information, related financial technology functions, research, data hosting, auditing, and data processing;
- Financial services companies (such as your custodian, brokers, or dealers) who effect transactions on your behalf;
- Companies participating with Envestnet in a proposed or actual sale, merger, transfer, or business exchange;
- Companies that participate in joint marketing activities with us;
- Non-affiliated parties as allowed by law, such as in responding to a subpoena, preventing fraud, or complying with an inquiry by a government agency or regulator; and
- Other organizations as directed by you or your representative.

Envestnet has disclosed one or more of the following categories of personal information for a business purpose in the preceding twelve (12) months to a party(ies) identified in this section: identifiers, customer records, classification characteristics, commercial information, Internet or other similar network activity, geolocation data, sensory data, professional or employment-related information, and inferences drawn from other personal information.

### **Retaining Personal Information**

Envestnet complies with financial laws and regulations to maintain records for statutorily required periods of time. Retaining personal information is often necessary for us and our service provider(s) to:

- Complete the transactions for which we collected the information, provide a requested good or service, take actions reasonably anticipated within the context of our ongoing business relationships, or otherwise perform our contract with you or on your behalf;



- Enable solely internal uses that are reasonably aligned with consumer expectations based on their relationship with us;
- Comply with a legal obligation, including but not limited to maintaining a books and records requirement under the Securities and Exchange Commission (SEC);
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- Debug products to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law; and
- Make other internal and lawful uses of that information that are compatible with the context in which the information was provided.

## **Protecting Collected Information**

We maintain security measures to safeguard against loss, theft, interference, and misuse, as well as unauthorized access, disclosure, alteration, or destruction of information. We also maintain procedures to help maintain the security of online sessions and to protect Envestnet accounts and systems. This approach helps ensure that information remains safe and private; however, you should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100 percent secure, accurate, complete, or current.

## **Notification of Changes**

By using the Services, you consent to the collection and use of the personal information described above. Envestnet reviews the Privacy Policy annually and reserves the right to amend the Privacy Policy at our discretion and at any time. Should we update the Privacy Policy, we will post those changes on this page with an updated effective date. Your continued use of the Services following the new effective date constitutes your consent to and acceptance of such changes.

## **Your Rights and Choices**

This Privacy Policy constitutes Envestnet disclosing to you Envestnet's collection, use, and disclosure of personal information for a business purpose over the past twelve (12) months. You may be entitled, in accordance with applicable laws, to request access to, deletion, and portability of your information or more information about our information practices. Requests should be submitted via e-mail [todayprivacyoffice@investnet.com](mailto:todayprivacyoffice@investnet.com). We will not discriminate against you for exercising your rights, although some of the functionality and features available on the Services may change or no longer be available to you. If your information is provided by your Representative or a third party, we may ask you to work with them in the removal of your information from the Services. Any difference in the Services or product requested is related to the value provided.

Once we receive your request, we may verify it by requesting information sufficient to confirm your identity. You may be entitled, in accordance with applicable laws, to submit a request through an authorized agent. To designate an authorized agent to exercise choices on your behalf, please provide evidence that you have given such agent power of attorney or that the agent otherwise has valid written authority to submit requests to exercise rights on your behalf.

If you have additional questions about the use of your data, you may reach out to your financial advisor or other Representative or contact Envestnet.

## International Customers

Our Services are hosted in the United States. If you are an international consumer, note that by providing your personal information, you are: (i) permitting the transfer of your personal information to the United States which may not have the same data protection laws as the country in which you reside; and (ii) permitting the use of your personal information in accordance with the Privacy Policy.

---

## CONTROL ENVIRONMENT

The control environment at Envestnet is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors and operations management.

### Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Envestnet's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Envestnet's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Specific control activities that the service organization has implemented are described below:

- A code of conduct is in place within the employee handbook to communicate entity values and behavioral standards to personnel.
- Employees are required to acknowledge their receipt of the code of conduct upon hire indicating that they have been given access to the code of conduct and understand their responsibility for adhering to the entity's commitments.
- Employees are required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- Background checks are performed for employees as a component of the hiring process.

### Board of Directors Oversight

Envestnet's control consciousness is influenced by its board of directors. The board of directors provides strategic direction and operational guidance, approves significant Envestnet acquisitions, and reviews and approves corporate plans and policies. Attributes include the board of directors' independence from management, the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. Specific control activities that the service organization has implemented in this area are described below:

- Corporate governance board bylaws are established which describe the responsibilities of the board of directors including oversight of management's system of internal control.
- The board of directors has a majority of members who are independent from management and are objective in evaluations and decision making.
- The board of directors meets on a quarterly basis to review and approve strategic company objectives.

## **Organizational Structure and Assignment of Authority and Responsibility**

Envestnet's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Envestnet's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Envestnet has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. The charts are updated as needed and communicated to employees via the Workday system. Additionally, documented position descriptions are in place to define the authorities and responsibilities required for employment positions.

## **Commitment to Competence**

Management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Envestnet's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Specific control activities that the service organization has implemented in this area are described below:

- Background check screening procedures and position descriptions are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- Professional development opportunities are available to employees through the following programs:
  - Learning management system;
  - Tuition reimbursement program; and
  - Career advancement and promotion policy.
- An employee referral program is in place to attract new talent and retain individuals who are invested in their peers and community.
- A performance review of employees is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.
- A compensation committee is in place to support the governance of incentive-based compensation.

## **Accountability**

The organization has defined accountability as holding individuals accountable for internal control responsibilities. Accountability encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitude toward information processing, accounting functions, and personnel. Specific control activities that the service organization has implemented in this area are described below.

- An employee sanction procedure is in place to communicate that an employee may be terminated for noncompliance with a policy and/or procedure.
- A performance review of employees is conducted on an annual basis and the results are documented and maintained in the employee's personnel file to hold individuals accountable for their internal control responsibilities.
- Employees are required to complete security awareness training upon hire and at least annually thereafter to confirm their understanding regarding their internal control responsibilities.

---

## RISK ASSESSMENT

Enterprise risk is defined as any significant event or circumstance which could impact the achievement of Envestnet's business objectives, including strategic, reporting (including financial), operational, technology, data security, business continuity, legal, and compliance risks.

Envestnet has an established risk management program that is facilitated by a cross-functional risk management committee (RMC) responsible for supervising the enterprise risk framework for the company. The RMC is chaired by the chief compliance officer and is comprised of over 40 senior level management representatives from various disciplines within the company and other members as determined by the RMC chairperson.

The primary responsibility of the RMC is to ensure that sound policies, procedures, and practices are in place for the enterprise-wide management of the company's material risks and to report the results of the RMC's activities to senior management and the company's board of directors. More specifically, the RMC:

- Designs and implements risk management practices by:
  - Providing ongoing guidance and support for the refinement of the overall risk management framework ensuring best practices are incorporated;
  - Ensuring that risk assessments are performed periodically and completely and that results are communicated to relevant stakeholders, senior management, and the board of directors; and
  - Ensuring that management understands and accepts its responsibility for: identifying hazards; assessing and categorizing the risk; evaluating existing controls; recommending additional risk controls; establishing acceptance criteria; and, for ongoing monitoring and reviewing of risks.
- Executes and monitors risk management practices by:
  - Approving company-wide risk assessment(s), including scope and frequency;
  - Determining which enterprise risks are most significant and assisting in the determination of resource allocation for risk monitoring and improvement activities;
  - Assigning risk owners and approving action plans on a periodic basis;
  - Reviewing and monitoring the progress of risk mitigation; and
  - Reviewing and reporting on a quarterly basis to the company's senior management and board of directors:
    - The magnitude of material business risks;
    - The processes, procedures, and controls in place to manage material risks; and
    - The overall effectiveness of the risk management process.

### Objective Setting

Management specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives including the following activities:

- The entity's objectives are documented to align with the company mission and enable the identification and assessment of risks.
- A documented risk assessment methodology is in place to guide personnel in identifying and analyzing risks relating to the documented objectives.
- A limited risk assessment is performed on a quarterly basis that considers the identification and assessment of risks relating to the documented objectives.

## Risk Identification and Analysis

The RMC meets as frequently as it deems necessary to carry out its duties and responsibilities but at least annually. The RMC provides oversight in achieving its enterprise-wide risk management vision and mission through reviewing, assessing, and discussing any significant risks or exposure and steps taken to minimize identified risks or exposures. The RMC helps achieve this vision by creating a comprehensive approach to anticipate, identify, prioritize, and manage material risks to Envestnet's business objectives.

The first phase in the risk assessment process is the identification of the assets within scope, i.e., those assets which may affect the confidentiality, integrity, and availability of information in the organization. Assets may be categorized as people, places, systems, data, processes, or intellectual property. When identifying assets, it is also necessary to identify their owners, i.e., the person or organizational unit responsible for each asset. An asset's value is determined by looking at the potential impact on the organization if the information asset were to be compromised. Information is first classified by type, then for each type of information the potential impact is rated on a four-tiered scale of very high, high, medium, and low for each of the three security objectives: confidentiality, integrity, and availability.

The next phase is to perform the risk assessment against a set of threats and vulnerabilities identified as applicable to the information and service assets in the organization. The risk assessment is completed in four stages, with one limited risk assessment performed during each fiscal quarter. A limited risk assessment evaluates one quarter of the identified risks so that each individual risk is evaluated on at least an annual basis. The risk owners, in conjunction with the RMC, add key information for each risk which include, but are not limited to, the following: risk title, objective, takeaways, risk owner, outlook, risk appetite, and risk score. During the limited risk assessment process, the list of controls which are not implemented are identified. Corresponding to each threat the corresponding business impact and probability of occurrence are calculated based on the following tables:

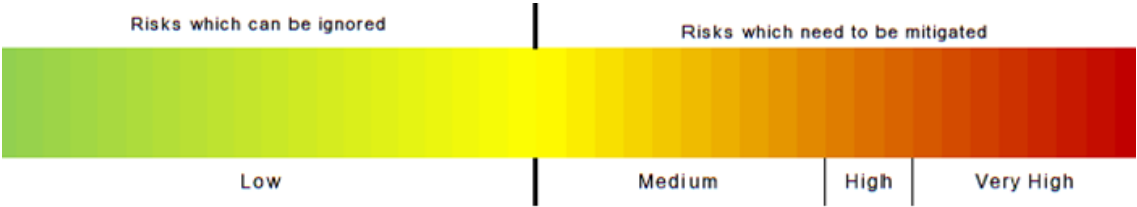
Business Impact		
Category	Criteria	
	Score	Definition
Catastrophic	1	May include: significant financial loss; inability to resume operations and services; significant client loss; long-term reputational damage.
Significant	0.75	May include: financial losses of \$1 million or more; reprioritizing of delivery required; moderate to high legal or compliance concern; likelihood of reputational damage.
Moderate	0.5	May include: financial loss, renegotiation of customer deadlines; SLAs not met; medium reputational damage; legal implications; risk of successful legal challenge.
Minor	0.25	May include: minor financial loss; little legal or compliance concern; minor reputational damage; potential business or platform disruption or loss of client confidence; non-systemic.
Insignificant	0.1	May include: small financial loss; no legal or compliance concern; limited reputational damage; inconsequential or easily recoverable business or platform issues.

Probability of Occurrence		
Category	Criteria	
	Score	Definition
Highly Probable	1	Certain to occur within the next year.
Probable	0.75	Almost certain to occur once within the next year.
Possible	0.5	May occur once in the next year.
Unlikely	0.25	Not likely to occur in the next year.
Rare	0.1	Not likely to occur within the next 5 years.

The risk value is calculated as a function of asset value, business impact, and probability of occurrence as follows:

Risk Valuation	
Risk Value = (Asset Value + Business Impact + Probability of Occurrence) / 3	

The risks are graded into very high, high, medium, and low. Risks which are graded as medium or above require risk mitigation.



**Risk Factors**

Management considers risks that can arise from both external and internal factors including the following:

*External Factors*

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

*Internal Factors*

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

**Potential for Fraud**

A documented risk assessment methodology is in place to guide personnel in identifying and assessing risks including the potential for fraud. The risk assessment considers the potential for fraud. Risks related to fraud are identified at least annually during the limited quarterly risk assessments and rated using a risk evaluation process and are documented for management review.

## Risk Mitigation

Risk is addressed in one of the following four methods:

- Risk Acceptance – No additional action is required. The organization decides that the associated risk is at an acceptable level, or the resources required to reduce the risk are more costly than the potential impact.
- Risk Mitigation – The implementation of countermeasures or security controls to reduce/eliminate a vulnerability or reduce the probability of likelihood.
- Risk Transfer – Engage in an agreement whereby the risk is borne by another entity (e.g., insurance).
- Risk Avoidance – The elimination of risk through the discontinuation of activities that have been determined to create risk.

A suitable plan to mitigate the risk is identified by the information owner and implemented. A person or team is identified to implement the mitigation plan. The target date for getting the mitigation plan implemented by the identified owner is also determined.

### *Vendor Risk Management*

Envestnet has established a vendor management policy to address risks associated with vendors and business partners that includes security within supplier agreements and monitoring and reviewing of suppliers. Additionally, the risk assessment considers risks associated with vendors and business partners. IT management reviews documentation provided by critical third-party vendors on an annual basis to help ensure that critical third-party vendors are in compliance with Envestnet's system requirements. Envestnet considers a third-party vendor to be critical if the vendor hosts customer data. Review of subservice organizations may include any of the following: reviewing security compliance reports (such as SOC reports); performing follow-up assessments based on the identified risk level; and performing an audit or assessment of subservice organization services.

---

## TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

### Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, processing integrity, confidentiality, and privacy categories.

### Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Envestnet's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

### Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criteria presented below are not applicable to the UMP system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the



omitted applicable trust services criteria. The following table presents the trust services criteria that are not applicable for the UMP system at Envestnet. The not applicable trust services criteria are also described within Section 4.

Criteria #	Reason for Omitted Criteria
P1.1	Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Envestnet given its role as a data processor.
P2.1	Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.
P3.2	Obtaining consent and communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.
P5.1	Providing access to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.
P5.2	Correcting, amending, or appending personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.
P6.1	Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Envestnet given its role as a data processor.
P6.7	Providing an accounting to the data subject of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.
P7.1	Collecting and maintaining accurate, up-to-date, complete, and relevant personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.

## INFORMATION AND COMMUNICATION SYSTEMS

Documented policies and procedures are in place that identify the information required to support the functioning of internal control and achievement of objectives. Information is necessary for Envestnet to carry out internal control responsibilities to support the achievement of its objectives related to the in-scope systems. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of internal control that include monitoring tools, industry publications, and internal assessments. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business.

Effective communication also must occur in a broader sense, flowing down, across, and up the organization. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

### *Internal Communications*

Documented policies and procedures are in place to guide personnel in the entity's commitments and the associated system requirements to support the functioning of internal control. The policies and procedures are communicated to internal personnel via the company intranet. Envestnet has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are conveyed. These methods include orientation and training for new employees, ongoing training for employees, communication of policies and procedures, including incident response and escalation, and the use of



e-mail to deliver time-sensitive information. Upon hire and at least annually thereafter, employees are required to complete security awareness training to confirm their understanding regarding their responsibilities for internal control. Additionally, documented position descriptions are in place to define the responsibilities for internal control. Documented escalation procedures for reporting incidents are provided to internal users to guide users in identifying and reporting failures, incidents, concerns, and other complaints.

### *External Communications*

Envestnet has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their services and communication of significant events. These methods include documenting the entity's commitments and the associated system requirements in standard customer contracts and company policies and procedures and establishing a help portal for external parties to report incidents, concerns, and complaints. A tracking system is utilized to document and track correspondence with external parties regarding matters affecting the functioning of internal control. Documented policies and procedures are in place to guide personnel in facilitating external communications. Envestnet's privacy policies and terms of use are available via Envestnet's public website.

---

## **MONITORING**

Monitoring is a process that assesses the quality of internal control performance over time; it involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties, such as user entity complaints and regulatory comments, that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

### Ongoing Monitoring

Envestnet's information security team performs continuous monitoring and testing of controls throughout the year to evaluate the ongoing operating effectiveness of the internal controls, including the following:

- In carrying out its regular management activities, operations management obtains evidence that the system of internal control continues to function, including error and performance reports.
- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Training, planning sessions, and other meetings provide important feedback to management on whether controls are effective.
- A SIEM application is utilized to monitor system events and alert IT personnel when certain predefined events occur.
- Antivirus software is utilized to detect and protect registered workstations and production servers from malicious activities.
- An IDS is utilized to analyze and report network events.

### Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy, management change, or significant changes in operations. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. The internal audit program comprises internal controls testing across various functions such as information technology, finance and accounting, operations, governance and compliance, and strategy and planning. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often. The internal audit testing is performed on an annual basis to ascertain whether the components of internal control are present and functioning. The internal audit plan and results are communicated to the audit committee for approval.

IT personnel perform external and internal vulnerability scans weekly, and a third-party vendor performs a penetration test on an annual basis. Issues that are identified as part of the vulnerability scans and penetration test are communicated to relevant parties, tracked, and monitored through resolution. The audit committee meets on a quarterly basis to further discuss internal control deficiencies to ensure that corrective action is taken.

#### Subservice Organization Monitoring

The services provided by Cyxtera are monitored on a regular basis as part of the day-to-day operations. On an annual basis, IT management reviews the SOC 1 and/or SOC 2 reports provided by Cyxtera to help ensure that the controls are suitably designed and operating effectively and that any relevant findings are sufficiently mitigated.

#### **Evaluating and Communicating Deficiencies**

Management has developed procedures to ensure findings of internal control deficiencies should be reported to operational management. This process enables individuals to provide needed support or oversight for taking corrective action and to communicate with others in the organization whose activities may be affected. Any deficiencies are investigated by management team members and, if necessary, are reported to the senior management team. Further, deficiencies are recorded and tracked through resolution via a ticketing system.

#### **System Incident Disclosures**

No system incidents occurred that were the result of controls that were not suitably designed or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements.

---

## **COMPLEMENTARY CONTROLS AT USER ENTITIES**

Envestnet's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

# SECTION 4

## TESTING MATRICES

## TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

### Scope of Testing

This report on the controls relates to the UMP system provided by Envestnet. The scope of the testing was restricted to the UMP system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period October 1, 2021, through September 30, 2022.

### Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

### Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

## Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

## Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the service commitments and system requirements, are presented in the “Subservice Organizations” section within Section 3.

## SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Control Environment</b>			
<b>CC1.1</b> COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	A code of conduct is in place within the employee handbook to communicate entity values and behavioral standards to personnel.	Inspected the employee handbook to determine that a code of conduct was in place within the employee handbook to communicate entity values and behavioral standards to personnel.	No exceptions noted.
CC1.1.2	Employees are required to acknowledge their receipt of the code of conduct upon hire indicating that they have been given access to the code of conduct and understand their responsibility for adhering to the entity's commitments.	Inspected the code of conduct acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged their receipt of the code of conduct upon hire indicating that they had been given access to the code of conduct and understood their responsibility for adhering to the entity's commitments.	The testing of the control activity disclosed that the code of conduct was not acknowledged upon hire for one of 25 employees sampled.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Employees are required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreement for a sample of employees hired during the period to determine that each employee sampled signed a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	No exceptions noted.
CC1.1.4	Background checks are performed for employees as a component of the hiring process.	Inspected the completed background check documentation for a sample of employees hired during the period to determine that background checks were performed for each employee sampled.	No exceptions noted.
<b>CC1.2</b> COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Corporate governance board bylaws are established which describe the responsibilities of the board of directors including oversight of management's system of internal control.	Inspected the corporate governance board bylaws to determine that corporate governance board bylaws were established which described the responsibilities of the board of directors including oversight of management's system of internal control.	No exceptions noted.
CC1.2.2	The board of directors has a majority of members who are independent from management and are objective in evaluations and decision making.	Inspected the board of directors' biographies to determine that the board of directors had a majority of members who were independent from management.	No exceptions noted.
CC1.2.3	The board of directors meets on a quarterly basis to review and approve strategic company objectives.	Inspected the board of directors meeting minutes for a sample of quarters during the period to determine that the board of directors met for each quarter sampled to review and approve strategic company objectives.	No exceptions noted.
<b>CC1.3</b> COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Organizational charts are in place that define the organizational structure, reporting lines, and authorities. These charts are communicated to employees and updated as needed.	Inspected the organizational charts on the company intranet to determine that organizational charts were in place that defined the organizational structure, reporting lines, and authorities and were communicated to employees and updated as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Documented position descriptions are in place that define the authorities and responsibilities required for employment positions.	Inspected the documented job descriptions for a sample of employment positions to determine that documented position descriptions were in place that defined the authorities and responsibilities required for each employment position sampled.	No exceptions noted.
<b>CC1.4</b> COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	An employee referral program is in place to attract new talent and retain individuals who are invested in their peers and community.	Inspected the employee handbook to determine that an employee referral program was in place to attract new talent and retain individuals who were invested in their peers and community.	No exceptions noted.
CC1.4.2	Background check screening procedures and position descriptions are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the background check summary procedure and an example job description to determine that background screening procedures and position descriptions were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.
CC1.4.3	Professional development opportunities are available to employees through the following programs: <ul style="list-style-type: none"> <li>• Learning management system</li> <li>• Tuition reimbursement program</li> <li>• Career advancement and promotion policy</li> </ul>	Inspected the development opportunity documentation to determine that professional development opportunities were available to employees through the following programs: <ul style="list-style-type: none"> <li>• Learning management system</li> <li>• Tuition reimbursement program</li> <li>• Career advancement and promotion policy</li> </ul>	No exceptions noted.
CC1.4.4	A performance review of employees is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.	Inspected the performance review for a sample of current employees to determine that a performance review was conducted for each employee sampled during the period to evaluate the performance of employees against expected levels of performance and conduct and provide opportunities for development as needed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.5	A compensation committee is in place to support the governance of incentive-based compensation.	Inspected the compensation committee charter to determine that a compensation committee was in place to support the governance of incentive-based compensation.	No exceptions noted.
<b>CC1.5</b> COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	An employee sanction procedure is in place to communicate that an employee may be terminated for noncompliance with a policy and/or procedure.	Inspected the information security policy to determine that an employee sanction procedure was in place to communicate that an employee may be terminated for noncompliance with a policy and/or procedure.	No exceptions noted.
CC1.5.2	A performance review of employees is conducted on an annual basis to evaluate the performance of employees against expected levels of performance and conduct and hold individuals accountable for their internal control responsibilities.	Inspected the performance review for a sample of current employees to determine that a performance review was conducted for each employee sampled during the period to evaluate the performance of employees against expected levels of performance and conduct and hold individuals accountable for their internal control responsibilities.	No exceptions noted.
CC1.5.3	Employees are required to complete security awareness training upon hire and at least annually thereafter to confirm their understanding regarding their internal control responsibilities.	Inspected the security awareness training roster for a sample of current and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding regarding their internal control responsibilities.	No exceptions noted.
<b>Communication and Information</b>			
<b>CC2.1</b> COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Documented policies and procedures are in place that identify the information required to support the functioning of internal control and achievement of objectives.	Inspected the information security policy to determine that documented policies and procedures were in place that identified the information required to support the functioning of internal control and achievement of objectives.	No exceptions noted.



Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	<p>Relevant and quality internal and external data sources are used to support the functioning of internal control that include, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>Monitoring tools</li> <li>Industry publications</li> <li>Internal assessments</li> </ul>	<p>Inspected example internal and external data source updates that occurred during the period to determine that relevant internal and external data sources were used to support the functioning of internal control that included the following:</p> <ul style="list-style-type: none"> <li>Monitoring tools</li> <li>Industry publications</li> <li>Internal assessments</li> </ul>	No exceptions noted.
<b>CC2.2</b> COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	<p>Documented policies and procedures are in place to guide personnel in the entity's commitments and the associated system requirements to support the functioning of internal control. The policies and procedures are communicated to internal personnel via the company intranet.</p>	<p>Inspected the policies and procedures posted on the company intranet to determine that documented policies and procedures were in place to guide personnel in the entity's commitments and the associated system requirements to support the functioning of internal control and were communicated to internal personnel via the company intranet.</p>	No exceptions noted.
CC2.2.2	<p>Documented position descriptions are in place to define the responsibilities for internal control.</p>	<p>Inspected the documented position descriptions for a sample of employment positions to determine that documented position descriptions were in place for each employment position sampled that defined the responsibilities for internal control.</p>	No exceptions noted.
CC2.2.3	<p>Documented escalation procedures are in place to guide internal personnel in identifying and reporting failures, incidents, concerns, and other complaints.</p>	<p>Inspected the incident response procedures to determine that documented escalation procedures were in place to guide internal personnel in identifying and reporting failures, incidents, concerns, and other complaints.</p>	No exceptions noted.
CC2.2.4	<p>Employees are required to complete security awareness training upon hire and at least annually thereafter to confirm their understanding regarding their internal control responsibilities.</p>	<p>Inspected the security awareness training roster for a sample of current and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding regarding their internal control responsibilities.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC2.3</b> COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Documented procedures are in place to guide personnel in communication with external parties regarding matters affecting the functioning of internal control.	Inspected the incident response procedures to determine that documented procedures were in place to guide personnel in communication with external parties regarding matters affecting the functioning of internal control.	No exceptions noted.
CC2.3.2	The entity's commitments and the associated system requirements are documented in customer agreements and company policies and procedures.	Inspected the commitments documentation to determine that the entity's commitments and the associated system requirements were documented in customer agreements and company policies and procedures.	No exceptions noted.
CC2.3.3	A tracking system is utilized to document and track correspondence with external parties regarding matters affecting the functioning of internal control.	Inspected the communications log to determine that a tracking system was utilized to document and track correspondence with external parties regarding matters affecting the functioning of internal control.	No exceptions noted.
CC2.3.4	A help portal is available to external parties to report security incidents, concerns, and complaints.	Inspected the help portal on the company website to determine that a help portal was available to external parties to report security incidents, concerns, and complaints.	No exceptions noted.
<b>Risk Assessment</b>			
<b>CC3.1</b> COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The entity's objectives are documented to align with the company mission and enable the identification and assessment of risks.	Inspected the objectives documentation to determine that the entity's objectives were documented to align with the company mission and enable the identification and assessment of risks.	No exceptions noted.
CC3.1.2	A limited risk assessment is performed on a quarterly basis that considers the identification and assessment of risks relating to the documented objectives.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered the identification and assessment of risks relating to the documented objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC3.2</b> COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	A documented risk assessment methodology is in place to guide personnel in identifying and analyzing risks relating to the documented objectives.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in identifying and analyzing risks relating to the documented objectives.	No exceptions noted.
CC3.2.2	A limited risk assessment is performed on a quarterly basis that considers the identification and assessment of risks relating to the documented objectives. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered the identification and assessment of risks relating to the documented objectives and that identified risks were rated using a risk evaluation process and were documented for management review.	No exceptions noted.
<b>CC3.3</b> COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A documented risk assessment methodology is in place to guide personnel in assessing risks including the potential for fraud.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in assessing risks including the potential for fraud.	No exceptions noted.
CC3.3.2	A limited risk assessment is performed on a quarterly basis that considers the potential for fraud. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered the potential for fraud and that identified risks were rated using a risk evaluation process and were documented for management review.	No exceptions noted.
<b>CC3.4</b> COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A documented risk assessment methodology is in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in identifying and assessing changes that could significantly impact the system of internal control.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	A limited risk assessment is performed on a quarterly basis that identifies and assesses changes that could significantly impact the system of internal control. Identified risks are rated using a risk evaluation process and are documented for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that identified and assessed changes that could significantly impact the system of internal control and that identified risks were rated using a risk evaluation process and were documented for management review.	No exceptions noted.
CC3.4.3	The entity's IT security group monitors the risks posed by emerging technologies and the impact of changes to applicable laws or regulations.	Inspected example security updates and notifications received during the period to determine that the entity's IT security group monitored the risks posed by emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
<b>Monitoring Activities</b>			
<b>CC4.1</b> COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis which include, but are not limited to, the following: <ul style="list-style-type: none"> <li>External vulnerability scans weekly</li> <li>Internal vulnerability scans weekly</li> <li>Penetration test annually</li> </ul>	Inspected the vulnerability assessment configurations and the most recent penetration test results to determine that security reviews and vulnerability assessments were performed by IT personnel and third-party vendors which included the following: <ul style="list-style-type: none"> <li>External vulnerability scans configured to initiate weekly</li> <li>Internal vulnerability scans configured to initiate weekly</li> <li>Penetration test during the period</li> </ul>	No exceptions noted.
CC4.1.2	The internal audit program is performed on an annual basis to ascertain whether the components of internal control are present and functioning. The internal audit plan and results are communicated to the audit committee for approval.	Inspected the most recent internal audit program results to determine that the internal audit program was performed during the period to ascertain whether the components of internal control were present and functioning.	No exceptions noted.
		Inspected the most recent audit committee meeting minutes and presentation to determine that the internal audit plan and results were communicated to the audit committee for approval.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC4.2</b> COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	<p>Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis which include, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>• External vulnerability scans weekly</li> <li>• Internal vulnerability scans weekly</li> <li>• Penetration test annually</li> </ul> <p>Identified issues are communicated to relevant parties, tracked, and monitored through resolution.</p>	<p>Inspected the vulnerability assessment configurations and the most recent penetration test results to determine that security reviews and vulnerability assessments were performed by IT personnel and third-party vendors which included the following:</p> <ul style="list-style-type: none"> <li>• External vulnerability scans configured to initiate weekly</li> <li>• Internal vulnerability scans configured to initiate weekly</li> <li>• Penetration test during the period</li> </ul>	No exceptions noted.
		<p>Inspected the remediation tracking documentation from the security assessments completed during the period to determine that identified issues were communicated to relevant parties, tracked, and monitored through resolution.</p>	No exceptions noted.
CC4.2.2	Meetings that include senior management participation are held on a quarterly basis to discuss internal control deficiencies to ensure that corrective action is taken.	Inspected the audit committee meeting minutes for a sample of quarters during the period to determine that meetings that included senior management participation were held for each quarter sampled to discuss internal control deficiencies.	No exceptions noted.
CC4.2.3	The internal audit program is performed on an annual basis to ascertain whether the components of internal control are present and functioning. The internal audit plan and results are communicated to the audit committee for approval.	Inspected the most recent internal audit program results to determine that the internal audit program was performed during the period to ascertain whether the components of internal control were present and functioning.	No exceptions noted.
		Inspected the most recent audit committee meeting minutes and presentation to determine that the internal audit plan and results were communicated to the audit committee for approval.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Control Activities</b>			
<b>CC5.1</b> COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A documented risk assessment methodology is in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks.	No exceptions noted.
CC5.1.2	A limited risk assessment is performed on a quarterly basis that considers the identification and assessment of risks relating to the documented objectives. Mitigation strategies that include the development of control activities are documented for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered the identification and assessment of risks relating to the documented objectives and that mitigation strategies that included the development of control activities were documented for management review.	No exceptions noted.
<b>CC5.2</b> COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	A documented risk assessment methodology is in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in selecting and developing general control activities over technology to support the achievement of objectives.	No exceptions noted.
CC5.2.2	A limited risk assessment is performed on a quarterly basis that considers the identification and assessment of risks relating to technology. Mitigation strategies that include the development of control activities over technology to support the achievement of objectives are documented for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered the identification and assessment of risks relating to technology and that mitigation strategies that included the development of control activities over technology to support the achievement of objectives were documented for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC5.3</b> COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Documented policies and procedures are in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems. These policies and procedures are communicated to internal personnel via the company intranet.	Inspected the information security policies posted on the company intranet to determine that documented policies and procedures were in place to guide personnel with regard to the design, development, implementation, operation, maintenance, and monitoring of the in-scope systems and were communicated to internal personnel via the company intranet.	No exceptions noted.
CC5.3.2	Employees are required to complete security awareness training upon hire and at least annually thereafter to confirm their understanding of their obligations and responsibilities to comply with the corporate security policies.	Inspected the security awareness training roster for a sample of current and new employees hired during the period to determine that each employee sampled completed security awareness training upon hire or during the period to confirm their understanding of their obligations and responsibilities to comply with the corporate security policies.	No exceptions noted.
<b>Logical and Physical Access Controls</b>			
<b>CC6.1</b> The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the in-scope system user account listings and minimum password requirements to determine that the in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	No exceptions noted.
CC6.1.2	Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the in-scope system user account listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
CC6.1.3	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the senior vice president (VP) of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC6.2</b> Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	User access requests are documented within the ticketing system and require manager approval.	Inspected the user access request ticket for a sample of employees hired during the period to determine that user access requests were documented within the ticketing system and approved by a manager for each employee sampled.	No exceptions noted.
CC6.2.2	A termination ticket is created and access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket and the in-scope user listings for a sample of employees terminated during the period to determine that a termination ticket was created and access was revoked for each terminated employee sampled.	No exceptions noted.
CC6.2.3	Privileged user access reviews are performed for the in-scope systems on a quarterly basis to help ensure that privileged access to systems is restricted.	Inspected the privileged user access review for a sample of quarters during the period to determine that privileged user access reviews were performed for the in-scope systems for each quarter sampled.	No exceptions noted.
<b>CC6.3</b> The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	User access requests are documented within the ticketing system and require manager approval.	Inspected the user access request ticket for a sample of employees hired during the period to determine that user access requests were documented within the ticketing system and approved by a manager for each employee sampled.	No exceptions noted.
CC6.3.2	A termination ticket is created and access is revoked for employees as a component of the employee termination process.	Inspected the termination ticket and the in-scope user listings for a sample of employees terminated during the period to determine that a termination ticket was created and access was revoked for each terminated employee sampled.	No exceptions noted.
CC6.3.3	Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the in-scope system user account listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.



Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the senior VP of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.5	Privileged user access reviews are performed for the in-scope systems on a quarterly basis to help ensure that privileged access to systems is restricted.	Inspected the privileged user access review for a sample of quarters during the period to determine that privileged user access reviews were performed for the in-scope systems for each quarter sampled.	No exceptions noted.
<b>CC6.4</b> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	Cyxtera is responsible for implementing controls to restrict physical access to facilities and protected information assets.		
<b>CC6.5</b> The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Documented policies are in place to guide personnel in the disposal of assets to ensure data and software is unrecoverable prior to retiring the physical asset.	Inspected the media sanitization and disposal policy to determine that documented policies were in place to guide personnel in the disposal of assets.	No exceptions noted.
CC6.5.2	Media containing customer data is sanitized or destroyed by a third party prior to the retiring of the physical asset.	Inquired of the manager of information security and inspected the asset disposal listing and determined that no media containing customer data was retired during the period; therefore, no testing of operating effectiveness was performed.	
<b>CC6.6</b> The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system configurations to determine that firewall systems were in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.
CC6.6.2	Encrypted VPN connections are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the VPN configurations to determine that encrypted VPN connections were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.6.3	Web servers utilize the transport layer security (TLS) encryption protocol for web communication sessions.	Inspected the encryption configurations to determine that web servers utilized the TLS encryption protocol for web communication sessions.	No exceptions noted.
CC6.6.4	An IDS is utilized to analyze and report network events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was utilized to analyze and report network events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC6.7</b> The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Documented policies are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the encryption policy to determine that documented policies were in place that prohibited the transmission of sensitive information over the Internet or other public communications paths unless it was encrypted.	No exceptions noted.
CC6.7.2	Encrypted VPN connections are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the VPN configurations to determine that encrypted VPN connections were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.7.3	Web servers utilize the TLS encryption protocol for web communication sessions.	Inspected the encryption configurations to determine that web servers utilized the TLS encryption protocol for web communication sessions.	No exceptions noted.
<b>CC6.8</b> The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Antivirus software is utilized to protect registered workstations and servers with the following configurations: <ul style="list-style-type: none"> <li>Scan for updates to antivirus definitions and update registered clients on a continuous basis</li> <li>Scan registered clients on a continuous basis</li> </ul>	Inspected the antivirus software configurations to determine that antivirus software was utilized to protect registered workstations and servers with the following configurations: <ul style="list-style-type: none"> <li>Scan for updates to antivirus definitions and update registered clients on a continuous basis</li> <li>Scan registered clients on a continuous basis</li> </ul>	No exceptions noted.
<b>System Operations</b>			
<b>CC7.1</b> To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis to identify new vulnerabilities and susceptibilities to new vulnerabilities which include, but are not limited to, the following: <ul style="list-style-type: none"> <li>External vulnerability scans weekly</li> <li>Internal vulnerability scans weekly</li> <li>Penetration test annually</li> </ul>	Inspected the vulnerability assessment configurations and the most recent penetration test results to determine that security reviews and vulnerability assessments were performed by IT personnel and third-party vendors to identify new vulnerabilities and susceptibilities to new vulnerabilities which included the following: <ul style="list-style-type: none"> <li>External vulnerability scans configured to initiate weekly</li> <li>Internal vulnerability scans configured to initiate weekly</li> <li>Penetration test during the period</li> </ul>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.2	A SIEM application is utilized to monitor system events and alert IT personnel via e-mail when certain predefined events occur.	Inspected the SIEM application configurations and an example alert generated during the period to determine that a SIEM application was utilized to monitor system events and alert IT personnel via e-mail when certain predefined events occurred.	No exceptions noted.
CC7.1.3	An IDS is utilized to analyze and report network events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was utilized to analyze and report network events.	No exceptions noted.
<b>CC7.2</b> The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Security reviews and vulnerability assessments are performed by IT personnel and third-party vendors on a periodic basis to identify anomalies which include, but are not limited to, the following: <ul style="list-style-type: none"> <li>• External vulnerability scans weekly</li> <li>• Internal vulnerability scans weekly</li> <li>• Penetration test annually</li> </ul>	Inspected the vulnerability assessment configurations and the most recent penetration test results to determine that security reviews and vulnerability assessments were performed by IT personnel and third-party vendors to identify anomalies which included the following: <ul style="list-style-type: none"> <li>• External vulnerability scans configured to initiate weekly</li> <li>• Internal vulnerability scans configured to initiate weekly</li> <li>• Penetration test during the period</li> </ul>	No exceptions noted.
CC7.2.2	A SIEM application is utilized to monitor system events to identify anomalies that are indicative of malicious acts, natural disasters, and errors and alert IT personnel via e-mail when certain predefined events occur.	Inspected the SIEM application configurations and an example alert generated during the period to determine that a SIEM application was utilized to monitor system events to identify anomalies that were indicative of malicious acts, natural disasters, and errors and alert IT personnel via e-mail when certain predefined events occurred.	No exceptions noted.
CC7.2.3	An IDS is utilized to analyze and report network events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was utilized to analyze and report network events.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.4	An enterprise monitoring application is utilized to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds are exceeded on monitored devices.	Inspected the enterprise monitoring application configurations and an example alert generated during the period to determine that an enterprise monitoring application was utilized to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
<b>CC7.3</b> The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Documented incident response and escalation procedures are in place to guide personnel in evaluating security events.	Inspected the information security incident management procedures to determine that documented incident response and escalation procedures were in place to guide personnel in evaluating security events.	No exceptions noted.
CC7.3.2	The information security management committee meets on a quarterly basis to evaluate potential security events and actions to prevent or address them.	Inspected the meeting minutes for a sample of quarters during the period to determine that the information security management committee met for each quarter sampled to evaluate potential security events and actions to prevent or address them.	No exceptions noted.
<b>CC7.4</b> The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented incident response and escalation procedures are in place to guide personnel in understanding, containing, remediating, and communicating security incidents.	Inspected the information security incident management procedures to determine that documented incident response and escalation procedures were in place to guide personnel in understanding, containing, remediating, and communicating security incidents.	No exceptions noted.
CC7.4.2	A tracking system is utilized to document security violations, responses, and resolution.	Inquired of the security manager regarding the security incident tracker to determine that a tracking system was utilized to document security violations, responses, and resolution.	No exceptions noted.
		Inspected the security incident tracker to determine that a tracking system was utilized to document security violations, responses, and resolution.	No exceptions noted.
CC7.4.3	The information security management committee meets on a quarterly basis to discuss incidents and corrective measures to ensure that incidents are contained and remediated.	Inspected the meeting minutes for a sample of quarters during the period to determine that the information security management committee met for each quarter sampled to discuss incidents and corrective measures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response and escalation procedures are in place to guide personnel in the identification, development, and implementation of activities to recover from identified security incidents.	Inspected the information security incident management procedures to determine that documented incident response and escalation procedures were in place to guide personnel in the identification, development, and implementation of activities to recover from identified security incidents.	No exceptions noted.
CC7.5.2	The information security management committee meets on a quarterly basis to discuss recovery strategies from identified incidents and threats.	Inspected the meeting minutes for a sample of quarters during the period to determine that the information security management committee met for each quarter sampled to discuss recovery strategies from identified incidents and threats.	No exceptions noted.
CC7.5.3	A root cause analysis is performed for incidents that includes an impact analysis, resolution, lessons learned, and action items.	Inquired of the security manager regarding the security incident tracker to determine that a root cause analysis was performed for incidents that included an impact analysis, resolution, lessons learned, and action items.	No exceptions noted.
		Inspected the security incident tracker to determine that a root cause analysis was performed for incidents and that it included an impact analysis, resolution, lessons learned, and action items.	No exceptions noted.
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Change management policies and procedures are in place that define documentation, testing, and approval requirements.	Inspected the change management policies and procedures to determine that change management policies and procedures were in place that defined documentation, testing, and approval requirements.	No exceptions noted.
CC8.1.2	A change management tracking system is utilized to centrally maintain, manage, and monitor change control activities.	Inspected the change documentation for a sample of changes implemented during the period to determine that a change management tracking system was utilized to centrally maintain, manage, and monitor each change sampled.	No exceptions noted.
CC8.1.3	Changes made to in-scope systems are authorized, tested when applicable, and approved.	Inspected the change documentation for a sample of changes implemented during the period to determine that each change sampled was authorized, tested when applicable, and approved.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.4	The production environment is logically segmented from the development and test environments.	Inspected the network diagram and server listing to determine that the production environment was logically segmented from the development and test environments.	No exceptions noted.
CC8.1.5	Patches are applied to production systems at least quarterly.	Inspected the patch change ticket for a sample of quarters during the period to determine that patches were applied to production systems for each quarter sampled.	No exceptions noted.
CC8.1.6	Version control software is utilized to restrict access to source code and provide rollback capabilities.	Inspected the version control software configurations and user listings to determine that version control software was utilized to restrict access to source code and provide rollback capabilities.	No exceptions noted.
CC8.1.7	The ability to promote changes into the production environment is segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with write access to source code and the listing of users with the ability to implement changes to determine that the ability to promote changes into the production environment was segregated from those with development responsibility and restricted to user accounts accessible by authorized personnel.	No exceptions noted.
<b>Risk Mitigation</b>			
<b>CC9.1</b> The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	A documented risk assessment methodology is in place to guide personnel in identifying, selecting, and developing risk mitigation activities for risks arising from potential business disruptions.	Inspected the risk assessment methodology to determine that a documented risk assessment methodology was in place to guide personnel in identifying, selecting, and developing risk mitigation activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	A limited risk assessment is performed on a quarterly basis that considers risks arising from potential business disruptions. Identified risks are rated using a risk evaluation process and are documented, along with mitigation strategies, for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered risks arising from potential business disruptions and that identified risks were rated using a risk evaluation process and were documented, along with mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>CC9.2</b> The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	<p>A vendor management policy is in place that addresses risks associated with vendors and business partners that includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> <li>• Security within supplier agreements</li> <li>• Monitoring and review of suppliers</li> </ul>	<p>Inspected the vendor management policy to determine that a vendor management policy was in place that addressed risks associated with vendors and business partners that included the following:</p> <ul style="list-style-type: none"> <li>• Security within supplier agreements</li> <li>• Monitoring and review of suppliers</li> </ul>	No exceptions noted.
CC9.2.2	A limited risk assessment is performed on a quarterly basis that considers risks associated with vendors and business partners. Identified risks are rated using a risk evaluation process and are documented, along with mitigation strategies, for management review.	Inspected the risk assessment documentation for a sample of quarters during the period to determine that a limited risk assessment was performed for each quarter sampled that considered risks associated with vendors and business partners and that identified risks were rated using a risk evaluation process and were documented, along with mitigation strategies, for management review.	No exceptions noted.
CC9.2.3	IT management reviews documentation provided by critical third-party vendors on an annual basis to help ensure that critical third-party vendors are in compliance with the organization's system requirements.	Inquired of the information assurance specialist regarding IT management's review of critical third-party vendors to determine that IT management reviewed documentation provided by critical third-party vendors on an annual basis to help ensure that critical third-party vendors were in compliance with the organization's system requirements.	No exceptions noted.
		Inspected the most recent vendor review documentation for a sample of critical third-party vendors to determine that IT management reviewed documentation provided by each critical third-party vendor sampled during the period.	No exceptions noted.

## ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>A1.1</b> The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	An enterprise monitoring application is utilized to monitor the in-scope system capacity levels to help enable the implementation of additional capacity when necessary and notify IT personnel via e-mail when predefined thresholds are exceeded on monitored devices.	Inquired of the senior database administrator regarding monitoring to determine that an enterprise monitoring application was utilized to monitor the in-scope system capacity levels to help enable the implementation of additional capacity when necessary.	No exceptions noted.
		Inspected the enterprise monitoring application configurations and an example alert generated during the period to determine that an enterprise monitoring application was utilized to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds were exceeded on monitored devices.	No exceptions noted.
<b>A1.2</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	An automated backup system is utilized to perform scheduled backups of production systems and data at predefined times.	Inspected the backup system configurations to determine that an automated backup system was configured to perform scheduled backups of production systems and data at predefined times.	No exceptions noted.
A1.2.2	The automated backup system is configured to notify IT personnel via e-mail regarding the failure of backup jobs.	Inspected the backup system configurations and an example e-mail alert notification generated during the period to determine that the automated backup system was configured to notify IT personnel via e-mail regarding the failure of backup jobs.	No exceptions noted.
A1.2.3	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	Inspected the business continuity and disaster recovery plans to determine that business continuity and disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
	Cyxtera is responsible for implementing controls to protect against environmental vulnerabilities and changing environmental conditions.		



Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>A1.3</b> The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	The disaster recovery plan is tested as a component of business continuity planning on an annual basis.	Inspected the business continuity plan progress report and most recent disaster recovery test results to determine that the disaster recovery plan was tested as a component of business continuity planning during the period.	No exceptions noted.

## ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>PI1.1</b> The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.			
PI1.1.1	System processes and interfaces are documented to describe the design and operation of the system and its boundaries.	Inspected the system process and interface documentation to determine that system processes and interfaces were documented to describe the design and operation of the system and its boundaries.	No exceptions noted.
PI1.1.2	The entity's commitments and the associated system requirements are documented in customer agreements and company policies and procedures.	Inspected the commitments documentation to determine that the entity's commitments and the associated system requirements were documented in customer agreements and company policies and procedures.	No exceptions noted.
PI1.1.3	Relevant and quality internal and external data sources are used to support the functioning of internal control that include, but are not limited to, the following: <ul style="list-style-type: none"> <li>Monitoring tools</li> <li>Industry publications</li> <li>Internal assessments</li> </ul>	Inspected example internal and external data source updates that occurred during the period to determine that relevant internal and external data sources were used to support the functioning of internal control that included the following: <ul style="list-style-type: none"> <li>Monitoring tools</li> <li>Industry publications</li> <li>Internal assessments</li> </ul>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>PI1.2</b> The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.			
PI1.2.1	The application is configured to automatically perform validation checks on data files to help ensure inputs are recorded completely and accurately.	Inspected the data validation configurations and results of an example transaction performed during the period to determine that the application was configured to automatically perform validation checks on data files.	No exceptions noted.
PI1.2.2	A SIEM application is utilized to monitor user-related events and provide an audit trail of data ingress activities.	Inspected the SIEM application configurations and an example alert generated during the period to determine that a SIEM application was utilized to monitor user-related events and provide an audit trail of data ingress activities.	No exceptions noted.
<b>PI1.3</b> The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.			
PI1.3.1	The application is configured to automatically perform validation checks on data files to help ensure data processed is complete and accurate.	Inspected the data validation configurations and results of an example transaction performed during the period to determine that the application was configured to automatically perform validation checks on data files.	No exceptions noted.
PI1.3.2	The application is configured to notify users via e-mail regarding identified errors. Identified application errors are tracked and monitored through resolution.	Inquired of the senior VP of technology services regarding error monitoring to determine that identified application errors were tracked and monitored through resolution.	No exceptions noted.
		Inspected the alerting configurations and an example e-mail alert generated during the period to determine that the application was configured to notify users via e-mail regarding identified errors.	No exceptions noted.
PI1.3.3	An enterprise monitoring application is utilized to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds are exceeded on monitored devices.	Inspected the enterprise monitoring application configurations and an example alert generated during the period to determine that an enterprise monitoring application was utilized to monitor the in-scope system capacity levels and notify IT personnel via e-mail when predefined thresholds were exceeded on monitored devices.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>PI1.4</b> The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.			
PI1.4.1	The application is configured to notify users via e-mail regarding identified errors to help ensure output is delivered accurately and timely. Identified application errors are tracked and monitored through resolution.	Inquired of the senior VP of technology services regarding error monitoring to determine that identified application errors were tracked and monitored through resolution.	No exceptions noted.
		Inspected the alerting configurations and an example e-mail alert generated during the period to determine that the application was configured to notify users via e-mail regarding identified errors.	No exceptions noted.
PI1.4.2	An automated backup system is utilized to perform scheduled backups of production systems and data at predefined times.	Inspected the backup system configurations to determine that an automated backup system was configured to perform scheduled backups of production systems and data at predefined times.	No exceptions noted.
PI1.4.3	The automated backup system is configured to notify IT personnel via e-mail regarding the failure of backup jobs.	Inspected the backup system configurations and an example e-mail alert notification generated during the period to determine that the automated backup system was configured to notify IT personnel via e-mail regarding the failure of backup jobs.	No exceptions noted.
<b>PI1.5</b> The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.			
PI1.5.1	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the senior VP of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
PI1.5.2	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the in-scope system user account listings and minimum password requirements to determine that the in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	No exceptions noted.
PI1.5.3	An automated backup system is utilized to perform scheduled backups of production systems and data at predefined times.	Inspected the backup system configurations to determine that an automated backup system was configured to perform scheduled backups of production systems and data at predefined times.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PI1.5.4	The automated backup system is configured to notify IT personnel via e-mail regarding the failure of backup jobs.	Inspected the backup system configurations and an example e-mail alert notification generated during the period to determine that the automated backup system was configured to notify IT personnel via e-mail regarding the failure of backup jobs.	No exceptions noted.

## ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>C1.1</b> The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Documented policies and procedures are in place to guide personnel in the retention of confidential information.	Inspected the data retention and destruction policies to determine that documented policies and procedures were in place to guide personnel in the retention of confidential information.	No exceptions noted.
C1.1.2	Confidential data is retained in accordance with established guidelines or contractual requirements.	Inquired of the VP of information security regarding data retention to determine that confidential data was retained in accordance with established guidelines or contractual requirements.	No exceptions noted.
		Inspected the database records for a sample of customers to determine that confidential data was retained in accordance with established guidelines or contractual requirements for each customer sampled.	No exceptions noted.
C1.1.3	Confidential data is stored in an encrypted format. Access to the encryption keys is restricted to authorized personnel.	Inspected the database encryption configurations and the encryption key user access listing with the assistance of the principal director of product SRE to determine that confidential data was stored in an encrypted format and that access to the encryption keys was restricted to authorized personnel.	No exceptions noted.
<b>C1.2</b> The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Documented policies and procedures are in place to guide personnel in the disposal of confidential data.	Inspected the data retention and destruction policies to determine that documented policies and procedures were in place to guide personnel in the disposal of confidential data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2.2	Confidential data is disposed of upon customer request and in accordance with contractual requirements.	Inquired of the VP of information security and inspected the listing of data disposal requests and determined that there was no confidential data requiring disposal during the period; therefore, no testing of operating effectiveness was performed.	

## ADDITIONAL CRITERIA FOR PRIVACY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy</b>			
<b>P1.1</b> The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.			
	Not applicable. Providing notice to data subjects regarding privacy practices, including changes in the use of personal information, is the responsibility of the data controller and not Envestnet given its role as a data processor.		
<b>Privacy Criteria Related to Choice and Consent</b>			
<b>P2.1</b> The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.			
	Not applicable. Communicating choice and obtaining consent regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.		
<b>Privacy Criteria Related to Collection</b>			
<b>P3.1</b> Personal information is collected consistent with the entity's objectives related to privacy.			
P3.1.1	The entity's objectives related to privacy including the methods of collecting personal information are documented and communicated externally.	Inspected the privacy policy posted on the company website to determine that the entity's objectives related to privacy including the methods of collecting personal information were documented and communicated externally.	No exceptions noted.
P3.1.2	A data classification policy is in place to identify personal information required to support the functioning of the services and associated protection, access rights, and disposal requirements.	Inspected the data classification policy to determine that a data classification policy was in place to identify personal information required to support the functioning of the services and associated protection, access rights, and disposal requirements.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P3.1.3	Employees are required to complete privacy training on an annual basis to understand their responsibility for complying with the privacy policy.	Inspected the privacy training documentation for a sample of current employees to determine that each employee sampled completed privacy training during the period to understand their responsibility for complying with the privacy policy.	No exceptions noted.
P3.1.4	A legal team is in place to provide legal guidance over the entity's personal information collection activities in accordance with documented roles and responsibilities.	Inspected the legal team runbook to determine that a legal team was in place to provide legal guidance over the entity's personal information collection activities in accordance with documented roles and responsibilities.	No exceptions noted.
<b>P3.2</b> For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.			
	Not applicable. Obtaining consent and communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information, to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.		
<b>Privacy Criteria Related to Use, Retention, and Disposal</b>			
<b>P4.1</b> The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.			
P4.1.1	The entity's objectives related to privacy including the use of personal information are documented and communicated externally.	Inspected the privacy policy posted on the company website to determine that the entity's objectives related to privacy including the use of personal information were documented and communicated externally.	No exceptions noted.
P4.1.2	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the senior VP of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
P4.1.3	Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the in-scope system user account listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
P4.1.4	The internal audit program is performed on an annual basis to ensure that the use of personal information is limited to the purposes identified in the entity's objectives related to privacy. The internal audit plan and results are communicated to the audit committee for approval.	Inspected the most recent internal audit program results to determine that the internal audit program was performed during the period that ensured the use of personal information was limited to the purposes identified in the entity's objectives related to privacy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the most recent audit committee meeting minutes and presentation to determine that the internal audit plan and results were communicated to the audit committee for approval.	No exceptions noted.
P4.1.5	Employees are required to complete privacy training on an annual basis to understand their responsibility for complying with the privacy policy.	Inspected the privacy training documentation for a sample of current employees to determine that each employee sampled completed privacy training during the period to understand their responsibility for complying with the privacy policy.	No exceptions noted.
<b>P4.2</b> The entity retains personal information consistent with the entity's objectives related to privacy.			
P4.2.1	Documented policies and procedures are in place to guide personnel in the retention of personal information.	Inspected the data retention and destruction policies to determine that documented policies and procedures were in place to guide personnel in the retention of personal information.	No exceptions noted.
P4.2.2	Personal information is retained in accordance with established guidelines or contractual requirements.	Inquired of the VP of information security regarding data retention to determine that personal information was retained in accordance with established guidelines or contractual requirements.	No exceptions noted.
		Inspected the database records for a sample of customers to determine that personal information was retained in accordance with established guidelines or contractual requirements for each customer sampled.	No exceptions noted.
P4.2.3	Personal information is stored in an encrypted format. Access to the encryption keys is restricted to authorized personnel.	Inspected the database encryption configurations and the encryption key user access listing with the assistance of the principal director of product SRE to determine that personal information was stored in an encrypted format and that access to the encryption keys was restricted to authorized personnel.	No exceptions noted.
<b>P4.3</b> The entity securely disposes of personal information to meet the entity's objectives related to privacy.			
P4.3.1	Documented policies and procedures are in place to guide personnel in the disposal of personal information.	Inspected the data retention and destruction policies to determine that documented policies and procedures were in place to guide personnel in the disposal of personal information.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P4.3.2	Personal information is disposed of upon customer request and in accordance with contractual requirements.	Inquired of the VP of information security and inspected the listing of data disposal requests and determined that there was no personal information requiring disposal during the period; therefore, no testing of operating effectiveness was performed.	
Privacy Criteria Related to Access			
P5.1 The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.			
	Not applicable. Providing access to data subjects is the responsibility of the data controller and not Envestnet given its role as a data processor.		
P5.2 The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.			
	Not applicable. Correcting, amending, or appending personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.		
Privacy Criteria Related to Disclosure and Notification			
P6.1 The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.			
	Not applicable. Obtaining consent from data subjects for purposes of third-party disclosure is the responsibility of the controller and not Envestnet given its role as a data processor.		
P6.2 The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.			
P6.2.1	A SIEM application is utilized to monitor user-related events and provide an audit trail of data ingress activities.	Inspected the SIEM application configurations and an example alert generated during the period to determine that a SIEM application was utilized to monitor user-related events and provide an audit trail of data ingress activities.	No exceptions noted.
P6.2.2	User access requests are documented within the ticketing system and require manager approval.	Inspected the user access request ticket for a sample of employees hired during the period to determine that user access requests were documented within the ticketing system and approved by a manager for each employee sampled.	No exceptions noted.
P6.2.3	An access request register is utilized to document and track authorized disclosures of personal information.	Inspected the access request register and personal data access request procedures to determine that an access request register was utilized to document and track authorized disclosures of personal information.	No exceptions noted.



Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
P6.2.4	The internal audit program is performed on an annual basis to ensure that a complete, accurate, and timely record of authorized disclosures is created and retained. The internal audit plan and results are communicated to the audit committee for approval.	Inspected the most recent internal audit program results to determine that the internal audit program was performed during the period that ensured a complete, accurate, and timely record of authorized disclosures was created and retained.	No exceptions noted.
		Inspected the most recent audit committee meeting minutes and presentation to determine that the internal audit plan and results were communicated to the audit committee for approval.	No exceptions noted.
<b>P6.3</b> The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.			
P6.3.1	A security incident log is maintained to track detected or reported unauthorized disclosures of personal information in accordance with the entity's objectives related to privacy.	Inquired of the VP of operations regarding the security incident tracker to determine that a security incident log was maintained to track detected or reported unauthorized disclosures of personal information in accordance with the entity's objectives related to privacy.	No exceptions noted.
		Inspected the security incident tracker to determine that a security incident log was maintained to track detected or reported unauthorized disclosures of personal information.	No exceptions noted.
P6.3.2	The information security management committee meets on a quarterly basis to evaluate potential security events and actions to prevent or address them.	Inspected the meeting minutes for a sample of quarters during the period to determine that the information security management committee met for each quarter sampled to evaluate potential security events and actions to prevent or address them.	No exceptions noted.
P6.3.3	Documented incident response and escalation procedures are in place to guide personnel in the identification, development, and implementation of activities to recover from detected or reported unauthorized disclosures of personal information.	Inspected the information security incident management procedures to determine that documented incident response and escalation procedures were in place to guide personnel in the identification, development, and implementation of activities to recover from detected or reported unauthorized disclosures of personal information.	No exceptions noted.
P6.3.4	A SIEM application is utilized to monitor user-related events and provide an audit trail of data ingress activities.	Inspected the SIEM application configurations and an example alert generated during the period to determine that a SIEM application was utilized to monitor user-related events and provide an audit trail of data ingress activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>P6.4</b> The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.			
P6.4.1	A supplier agreement is in place that stipulates the requirements for information security and privacy for vendors and third parties.	Inspected the supplier agreement to determine that a supplier agreement was in place that stipulated the requirements for information security and privacy for vendors and third parties.	No exceptions noted.
P6.4.2	IT management reviews documentation provided by critical third-party vendors on an annual basis to help ensure that critical third-party vendors are in compliance with the organization's system requirements.	Inquired of the information assurance specialist regarding IT management's review of critical third-party vendors to determine that IT management reviewed documentation provided by critical third-party vendors on an annual basis to help ensure that critical third-party vendors were in compliance with the organization's system requirements.	No exceptions noted.
		Inspected the most recent vendor review documentation for a sample of critical third-party vendors to determine that IT management reviewed documentation provided by each critical third-party vendor sampled during the period.	No exceptions noted.
<b>P6.5</b> The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.			
P6.5.1	A supplier agreement is in place that stipulates the requirements for vendors and third parties to notify the organization in the event of an actual or suspected unauthorized data disclosure.	Inspected the supplier agreement to determine that a supplier agreement was in place that stipulated the requirements for vendors and third parties to notify the organization in the event of an actual or suspected unauthorized data disclosure.	No exceptions noted.
P6.5.2	A security incident log is maintained to track actual or suspected unauthorized disclosures of personal information including notifications received from vendors and third parties and the response in accordance with the entity's objectives related to privacy.	Inquired of the VP of operations regarding the security incident tracker to determine that a security incident log was maintained to track actual or suspected unauthorized disclosures of personal information including notifications received from vendors and third parties and the response in accordance with the entity's objectives related to privacy.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security incident tracker to determine that a security incident log was maintained to track actual or suspected unauthorized disclosures of personal information.	No exceptions noted.
P6.5.3	Documented incident response and escalation procedures are in place to guide personnel in the identification, development, and implementation of activities to recover from detected or reported unauthorized disclosures of personal information.	Inspected the information security incident management procedures to determine that documented incident response and escalation procedures were in place to guide personnel in the identification, development, and implementation of activities to recover from detected or reported unauthorized disclosures of personal information.	No exceptions noted.
<b>P6.6</b> The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.			
P6.6.1	Documented incident response and escalation procedures are in place to guide personnel in requirements for the notification of unauthorized disclosures of personal information to customers, regulators, and other affected parties.	Inspected the information security incident management procedures and breach notification template to determine that documented incident response and escalation procedures were in place to guide personnel in requirements for the notification of unauthorized disclosures of personal information to customers, regulators, and other affected parties.	No exceptions noted.
P6.6.2	A security incident log is maintained to track unauthorized disclosures of personal information in accordance with the entity's objectives related to privacy.	Inquired of the VP of operations regarding the security incident tracker to determine that a security incident log was maintained to track unauthorized disclosures of personal information in accordance with the entity's objectives related to privacy.	No exceptions noted.
		Inspected the security incident tracker to determine that a security incident log was maintained to track unauthorized disclosures of personal information.	No exceptions noted.
P6.6.3	The information security management committee meets on a quarterly basis to evaluate relevant data privacy laws impacting the use of personal information and actions required for compliance with the regulations.	Inspected the meeting minutes for a sample of quarters during the period to determine that the information security management committee met for each quarter sampled to evaluate relevant data privacy laws impacting the use of personal information and actions required for compliance with the regulations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>P6.7</b> The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.			
	Not applicable. Providing an accounting to the data subject of the personal information held and disclosing a data subject's personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.		
<b>Privacy Criteria Related to Quality</b>			
<b>P7.1</b> The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.			
	Not applicable. Collecting and maintaining accurate, up-to-date, complete, and relevant personal information is the responsibility of the data controller and not Envestnet given its role as a data processor.		
<b>Privacy Criteria Related to Monitoring and Enforcement</b>			
<b>P8.1</b> The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.			
P8.1.1	Personal information handling policies and procedures are in place to guide personnel in receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes.	Inspected the personal information handling policies and procedures to determine that personal information handling policies and procedures were in place to guide personnel in receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes.	No exceptions noted.
P8.1.2	A monitored e-mail account is utilized for submitting inquiries, complaints, and disputes regarding the entity's collection and use of personal information.	Inspected the privacy policy posted on the company website and e-mail configurations to determine that a monitored e-mail account was utilized for submitting inquiries, complaints, and disputes regarding the entity's collection and use of personal information.	No exceptions noted.
P8.1.3	An access request register is utilized to document and track inquires, complaints, disputes from initiation through resolution.	Inspected the access request register and personal data access request procedures to determine that an access request register was utilized to document and track inquires, complaints, and disputes from initiation through resolution.	No exceptions noted.
P8.1.4	The organization responds to data access requests as a result of inquiries, complaints, and disputes within predefined timeframes.	Inspected the data access request documentation for a sample of data access and modification requests received during the period to determine that the organization responded to each data access request sampled within predefined timeframes.	No exceptions noted.

## PRIVACY NOTICE COMMITMENTS

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>We do not sell consumer personal information about a current or former account to third parties.</b>			
PC1.1	The entity's objectives related to privacy including the use of personal information are documented and communicated externally.	Inspected the privacy policy posted on the company website to determine that the entity's objectives related to privacy including the use of personal information were documented and communicated externally.	No exceptions noted.
PC1.2	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the VP of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
PC1.3	Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the in-scope system user account listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
PC1.4	The internal audit program is performed on an annual basis to help ensure that personal information is not sold to third parties. The internal audit plan and results are communicated to the audit committee for approval.	Inspected the most recent internal audit program results to determine that the internal audit program was performed during the period that ensured personal information was not sold to third parties.	No exceptions noted.
		Inspected the most recent audit committee meeting minutes and presentation to determine that the internal audit plan and results were communicated to the audit committee for approval.	No exceptions noted.
PC1.5	Employees are required to complete privacy training on an annual basis to understand their responsibility for complying with the privacy policy.	Inspected the privacy training documentation for a sample of current employees to determine that each employee sampled completed privacy training during the period to understand their responsibility for complying with the privacy policy.	No exceptions noted.
<b>We comply with financial laws and regulations to maintain records for statutorily required periods of time.</b>			
PC2.1	Documented policies and procedures are in place to guide personnel in the retention of personal information.	Inspected the data retention and destruction policies to determine that documented policies and procedures were in place to guide personnel in the retention of personal information.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PC2.2	Personal information is retained in accordance with established guidelines or contractual requirements.	Inquired of the VP of information security regarding data retention to determine that personal information was retained in accordance with established guidelines or contractual requirements.	No exceptions noted.
		Inspected the database records for a sample of customers to determine that personal information was retained in accordance with established guidelines or contractual requirements for each customer sampled.	No exceptions noted.
PC2.3	Personal information is stored in an encrypted format. Access to the encryption keys is restricted to authorized personnel.	Inspected the database encryption configurations and the encryption key user access listing with the assistance of the principal director of product SRE to determine that personal information was stored in an encrypted format and that access to the encryption keys was restricted to authorized personnel.	No exceptions noted.
<b>We maintain security measures to safeguard against loss, theft, interference, and misuse, as well as unauthorized access, disclosure, alteration, or destruction of personal information.</b>			
PC3.1	The in-scope systems are configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	Inspected the in-scope system user account listings and minimum password requirements to determine that the in-scope systems were configured to authenticate users with a user account and enforce predefined user account and minimum password requirements.	No exceptions noted.
PC3.2	Predefined user groups are utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	Inspected the in-scope system user account listings to determine that predefined user groups were utilized to assign role-based access privileges and segregate access to data to the in-scope systems.	No exceptions noted.
PC3.3	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the in-scope system administrator listings with the assistance of the senior VP of systems to determine that administrative access privileges to the in-scope systems were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
PC3.4	Firewall systems are in place to filter unauthorized inbound network traffic from the Internet.	Inspected the firewall system configurations to determine that firewall systems were in place to filter unauthorized inbound network traffic from the Internet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
PC3.5	Encrypted VPN connections are utilized for remote access for the security and integrity of the data passing over the public network.	Inspected the VPN configurations to determine that encrypted VPN connections were utilized for remote access for the security and integrity of the data passing over the public network.	No exceptions noted.
PC3.6	Web servers utilize the TLS encryption protocol for web communication sessions.	Inspected the encryption configurations to determine that web servers utilized the TLS encryption protocol for web communication sessions.	No exceptions noted.
PC3.7	An IDS is utilized to analyze and report network events.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was utilized to analyze and report network events.	No exceptions noted.
	Cyxtera is responsible for implementing controls to restrict physical access to facilities and protected information assets.		
Should we make a material change to the Privacy Policy, we will post those changes on the company website with an updated effective date.			
PC4.1	The entity's objectives related to privacy including the methods of notifying users regarding material changes to the privacy policy are documented and communicated externally.	Inspected the privacy policy posted on the company website to determine that the entity's objectives related to privacy including the methods of notifying users regarding material changes to the privacy policy were documented and communicated externally.	No exceptions noted.
PC4.2	Users are notified of material changes to the privacy policy via the company website.	Inspected the website revision history to determine that users were notified of changes to the privacy policy via the company website.	No exceptions noted.

## **SECTION 5**

### **OTHER INFORMATION PROVIDED BY ENVESTNET**



## MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

### Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.2	Employees are required to acknowledge their receipt of the code of conduct upon hire indicating that they have been given access to the code of conduct and understand their responsibility for adhering to the entity's commitments.	Inspected the code of conduct acknowledgement for a sample of employees hired during the period to determine that each employee sampled acknowledged their receipt of the code of conduct upon hire indicating that they had been given access to the code of conduct and understood their responsibility for adhering to the entity's commitments.	The testing of the control activity disclosed that the code of conduct was not acknowledged upon hire for one of 25 employees sampled.
<b>Management's Response:</b>	The compliance desktop procedures have been modified to help ensure the completion of the initial compliance attestations. Managers are copied on emails regarding the compliance attestation process, and the new employee has 10 days to complete the required compliance attestations before it becomes a code of ethics violation.		

---

## **ADDITIONAL INFORMATION PROVIDED BY MANAGEMENT**

### **Building Security**

Envestnet offices are leased premises managed by their respective facility manager company independent of Envestnet. Building management retains the security personnel. After business hours, only those parties with electronic keycards/fobs issued by building management have elevator access to the floor containing the Envestnet offices. The electronic keycard limits access to the prescribed tenant's floor.

Depending on the location, a second keycard/fob/badge is required to enter the Envestnet office. After business hours, building access is limited to one control point at a security monitored entrance.

Envestnet has offices in Trivandrum, India. Security guards staffed on a 24x7 basis are placed in the reception lobby, access cards control the turnstiles, and the reception area is under closed circuit television (CCTV) surveillance. Access card readers and real-time surveillance is present throughout the perimeter: lobby, floor entrances, fire exits, white floors, data center uninterruptible power supply (UPS), for local offices, and electrical room. CCTV recordings are retained 90 days for internal cameras and three days for perimeter cameras.

For offices with a reception area, visitors are required to sign the visitors log and be escorted by an employee while in the office. For Trivandrum, visitors are also given a temporary badge without access cards. Temporary badges are logged in the visitor register.

### **Data Center Operations**

The Cyxtera data centers are staffed on a 24X7 basis. Security is provided at multiple checkpoints for entry which includes cameras and card key access with biometric scanners. The facilities themselves have redundant heating, ventilation, and air conditioning (HVAC) systems, electrical systems with battery backup, and diesel generators. Gas-charged fire suppressant systems are in place and the primary and alternate data centers are equipped with smoke and ionization detectors, CCTV monitoring, and temperature and other environment monitors.