linford&co llp cpa firm

Propelus

SOC 3

REPORT ON CONTROLS RELEVANT TO SECURITY AND CONFIDENTIALITY

NOVEMBER 1, 2023 TO OCTOBER 31, 2024

CE Broker, Inc. (dba) Propelus

Report on Propelus' Description of its CE Broker, EverCheck, and Immuware SaaS and Its Controls Relevant to Security and Confidentiality

Table of Contents

linford&co llp
cpa firm

▪ linford&co llp
1550 wewatta st, 2nd floor
denver, co 80202

▪ tel: +1 (720) 330 7201
email: info@linfordco.com
www.linfordco.com

Section I – Report of Independent Auditors

The Management of Propelus:

Scope

We have examined CE Broker, Inc., d/b/a Propelus' accompanying assertion titled "Assertion of Propelus' Management" (assertion) that the controls within Propelus' CE Broker, EverCheck, and Immuware Software as a Service (system) were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Propelus' service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Propelus 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 Propelus' service commitments and system requirements were achieved. Propelus has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Propelus is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that controls were not effective to achieve Propelus' service commitments and system requirements based on the applicable trust services criteria.

- ✓ Performing procedures to obtain evidence about whether the controls within the system were effective to achieve Propelus' service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Opinion

In our opinion, management's assertion that the controls within Propelus' CE Broker, EverCheck, and Immuware Software as a Service were effective throughout the period November 1, 2023 to October 31, 2024 to provide reasonable assurance that Propelus' service commitments and system requirements were achieved based on the applicable trust services criteria fairly stated, in all material respects.

linford&co llp

December 18, 2024
Denver, Colorado

Section II – Assertion of Propelus' Management

December 18, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Propelus' CE Broker, EverCheck, and Immuware Software as a Service (system) throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Propelus' service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Our description of the boundaries of the system is presented in Section III, and it identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Propelus' service commitments and system requirements were achieved based on the applicable trust services criteria. Propelus' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Propelus' service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/Aaron Prom
CAO & Counsel

Section III – Propelus' Description of Its CE Broker, EverCheck, and Immuware SaaS

Overview of Operations

CE Broker was founded in 2003 to provide a wide range of technology solutions and services to its clients, including the CE Broker, EverCheck, and Immuware SaaS. In April of 2023, CE Broker acquired Carminati Consulting (Immuware) and the entities merged into and with CE Broker, Inc., d/b/a Propelus, and were subsequently rebranded as Propelus. Propelus' mission is to deliver trusted and comprehensive technology solutions to propel the progress of dedicated professionals to advance their careers. Propelus delivers its mission through its CE Broker, EverCheck, and Immuware SaaS. The CE Broker, EverCheck, and Immuware SaaS are included in the scope of this report.

Description of Services

Infrastructure

The CE Broker, EverCheck, and Immuware SaaS are hosted in Microsoft Azure (Azure), Amazon Web Services (AWS), and Oracle Cloud (Oracle) and are delivered to end users as SaaS. Propelus has configured and utilizes various Azure, AWS, and Oracle security and performance monitoring tools, as well as Microsoft DevOps for managing the software development life cycle.

Software and Services

CE Broker SaaS
CE Broker is a continuing education solution for busy professionals to take, track, and report continuing education (CE) status to their boards. This product, coupled with the Evercheck product, allows organizations to better track and help their employees maintain their Certification and training requirements.

EverCheck SaaS
The EverCheck SaaS, also referred to as EverCheck One, is a web-based, multi-user service that provides low-touch, automated compliance solutions to satisfy human resources (HR) and education requirements within healthcare organizations. The EverCheck One platform supports healthcare organizations by:

- Enabling the daily automatic verification and tracking of healthcare licenses
- Enabling the collection and verification of licenses from employees prior to their start date
- Building and maintaining an ongoing history of licenses' status history for employees
- Building and maintaining an ongoing history of CE history for employees
- Meeting the primary source, license verification requirements for healthcare organizations set for by the joint commission

- Scheduling automatic notifications in the event an employee's license status changes or as license expiration dates approach
- Scheduling automated continuing education deadline and renewal reminders for healthcare employees
- Exporting licensing data to employer HR information system (HRIS) databases to provide automatic, up to date employee licensing status
- Tracking employee continuing education completion status and overviews of past due and coming due requirements
- Providing access to official up-to-date continuing education requirements
- Providing mobile solutions for employees to scan or capture license photos, upload licenses, enter license/eCardnumbers, validate the license, and send the data to employers automatically.

Employees' license and CE status, requirements, and renewal reminders are maintained by EverCheck One from pre-hire to post-hire. Healthcare employers send EverCheck their employees' current license or education information from the HRIS, which are imported into EverCheck One. Daily processes are run to perform the automated tracking and reporting on the employee requirements. System generated reports and reminders allow employers to gain visibility into the current compliance status of their employees. Information is shared with users via email, Secure File Transfer Protocol (SFTP), secure websites, and secure mobile applications.

Immuware SaaS

The Immuware SaaS enables end users to automate compliance workflows. Users directly access the CE Broker, EverCheck, and Immuware SaaS through user accounts with distinct permissions that correlate to functional responsibilities. Once authenticated to Immuware SaaS, users are able to view their compliance status and self-report required information remotely. The Immuware SaaS allows supervisors to monitor the compliance status of their personnel real-time and use automated notifications to follow up on missing requirements. Client administrators have elevated permissions to oversee processes, automate approval workflows, and automatically generate government-mandated reports and real-time reports for management.

Other key features of the Immuware SaaS include:

- A self-service portal to upload external documentation, pre-consent, and access to their record history
- Email and SMS notifications to personnel
- Consent via electronic signature
- Personnel declination and exemptions
- Required vs preferred compliance tracking by personnel, location, department, and job position
- Insight into upcoming, soon to expire, and expired compliance requirements via Immuware's Next Step and Expiring Queues
- The ability to view, report, download, and print individual personnel health history
- Automated administrator approval workflows

- The ability to view, export, and deliver the National Healthcare Safety Network (NHSN) and Occupational Safety and Health Administration (OSHA) formatted reports to support organizational compliance
- Access via Wi-Fi or cellular connection from any location
- Compatibility with computers, tablets, and mobile devices.

Data

Propelus' CE Broker, EverCheck, and Immuware SaaS collect and process various data in support of the services. In order to appropriately manage the data processed by and stored in the CE Broker, EverCheck, and Immuware SaaS, Propelus has implemented controls that apply a commensurate level of security throughout the data management life cycle, i.e., processing/transit, storage, and destruction.

Propelus is subject to certain laws and regulations, as well as contractual requirements. Under such laws, regulations, and requirements, Propelus takes measures to prevent unauthorized and inappropriate use or disclosure of confidential and sensitive data by implementing measures to safeguard the confidentiality, integrity, and availability of such data. These measures include training company personnel in information security matters, implementation of least principal access control measures, segregation of client data within the environment, encryption of sensitive data, and strong authentication mechanisms to Propelus systems.

Subservice Organizations

Propelus uses Azure, AWS, and Oracle for cloud infrastructure hosting and management services. The subservice organizations use an Infrastructure as a Service (IaaS) model to host the CE Broker, EverCheck, and Immuware SaaS and are responsible for maintaining the related physical and environmental controls and certain logical security and monitoring controls. The Azure, AWS, and Oracle services are subject to SOC 2 examinations at least annually. Propelus obtains and reviews the SOC 2 reports provided by the subservice organizations related to their hosting operations to determine whether controls are designed and operating effectively. Additionally, any complementary user entity controls listed in the SOC reports are reviewed and addressed by Propelus.

People

Propelus' personnel are organized into distinct functional areas with defined reporting lines to support the delivery of Propelus' services and its CE Broker, EverCheck, and Immuware SaaS. Additionally, Propelus has established a security team, which has been assigned ultimate responsibility for security and policy enforcement. The security team includes representation from company leadership and meets regularly to discuss threats, issues, remediation status, key risks, roadmaps, status, and to propose security policy changes.

Policies and Procedures

Propelus has established an internal control environment defined through its policies and procedures. The policies and procedures cover the following areas:

- Information security
- User access management
- Encryption standards
- Software development and change management
- Risk assessment and management
- Vulnerability management
- Systems monitoring and operational incident management
- Information security incident management
- Business continuity management and disaster recovery
- Code of conduct and ethics
- Data management

Policies and procedures are made available to company personnel to provide direction regarding responsibilities related to the functioning of internal control. Propelus also provides information to clients and company personnel on how to report failures, incidents, concerns, or complaints related to the services or systems provided by Propelus in the event there are problems and takes actions as appropriate when issues are raised.

Principal Service Commitments and System Requirements

Propelus designs its processes and procedures to meet objectives for its CE Broker, EverCheck, and Immuware SaaS. Those objectives are based on the service commitments that Propelus makes to user entities and the compliance requirements that Propelus has established for its services.

Security and confidentiality commitments to user entities are documented and communicated in their client agreements, as well as in the description of the service offering provided online. Security and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the CE Broker, EverCheck, and Immuware SaaS are implemented to permit system users access to the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the platform and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.
- Non-disclosure and confidentiality agreements with clients.

Propelus establishes operational requirements that support the achievement of security and confidentiality commitments and other system requirements. Such requirements are communicated in Propelus' policies and procedures, system design documentation, and contracts with clients. 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 networks are managed, and how personnel are screened, onboarded, and trained.

(The remainder of this page is left blank intentionally.)

Complementary Subservice Organization Controls (CSOC)

Propelus' controls related to the CE Broker, EverCheck, and Immuware SaaS cover only a portion of the overall system of internal control for each user entity of Propelus. It is not feasible for the applicable trust services criteria related to the CE Broker, EverCheck, and Immuware SaaS to be achieved solely by Propelus. Therefore, each user entity's internal controls must be evaluated in conjunction with Propelus' controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations, described as follows:

	Microsoft Azure Complementary Subservice Organization Controls
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.
3.	The subservice organization is responsible for maintaining 24/7/365 availability of the hosted environments.
4.	The subservice organization is responsible for monitoring the hosted environments and managing and resolving security and availability incidents and problems reported by Propelus in a timely manner.
5.	The subservice organization is responsible for implementing policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of each facility, and the movement of these items within the facility.

	AWS Complementary Subservice Organization Controls
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.
3.	The subservice organization is responsible for maintaining 24/7/365 availability of the hosted environments.

4.	The subservice organization is responsible for monitoring the hosted environments and managing and resolving security and availability incidents and problems reported by Propelus in a timely manner.
5.	The subservice organization is responsible for implementing policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of each facility, and the movement of these items within the facility.

	Oracle Cloud Complementary Subservice Organization Controls
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.
3.	The subservice organization is responsible for maintaining 24/7/365 availability of the hosted environments.
4.	The subservice organization is responsible for monitoring the hosted environments and managing and resolving security and availability incidents and problems reported by Propelus in a timely manner.
5.	The subservice organization is responsible for implementing policies and procedures that govern the receipt and removal of hardware and electronic media that contain sensitive information into and out of each facility, and the movement of these items within the facility.

(The remainder of this page is left blank intentionally.)

Propelus' Complementary User Entity Controls (CUEC)

Propelus' controls related to the CE Broker, EverCheck, and Immuware SaaS cover only a portion of the overall system of internal control for each user entity of Propelus. It is not feasible for the applicable trust services criteria related to the CE Broker, EverCheck, and Immuware SaaS to be achieved solely by Propelus. Therefore, each user entity's internal controls should be evaluated in conjunction with Propelus' controls, taking into account the related complementary user entity controls identified below.

This section highlights additional control activities that Propelus believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. User auditors should consider whether the following controls have been placed in operation at user organizations:

	Complementary User Entity Controls
1.	User entities are responsible for reporting known issues and security incidents through the specified communication channels.
2.	User entities are responsible for provisioning and de-provisioning users' access to the user entity's instance.
3.	User entities are responsible for configuring password parameters in the CE Broker, EverCheck, and Immuware SaaS for user entity accounts that align with industry standards.
4.	User entities are responsible for developing and testing an incident response plan for security incidents that occur within the user entity's environment.
5.	User entities are responsible for developing a disaster recovery plan for disaster scenarios that may impact the user entity's environment.
6.	User entities are responsible for performing backups of their data.
7.	User entities are responsible for making sure their methods of delivering data to Propelus conform with their own security and confidentiality requirements.