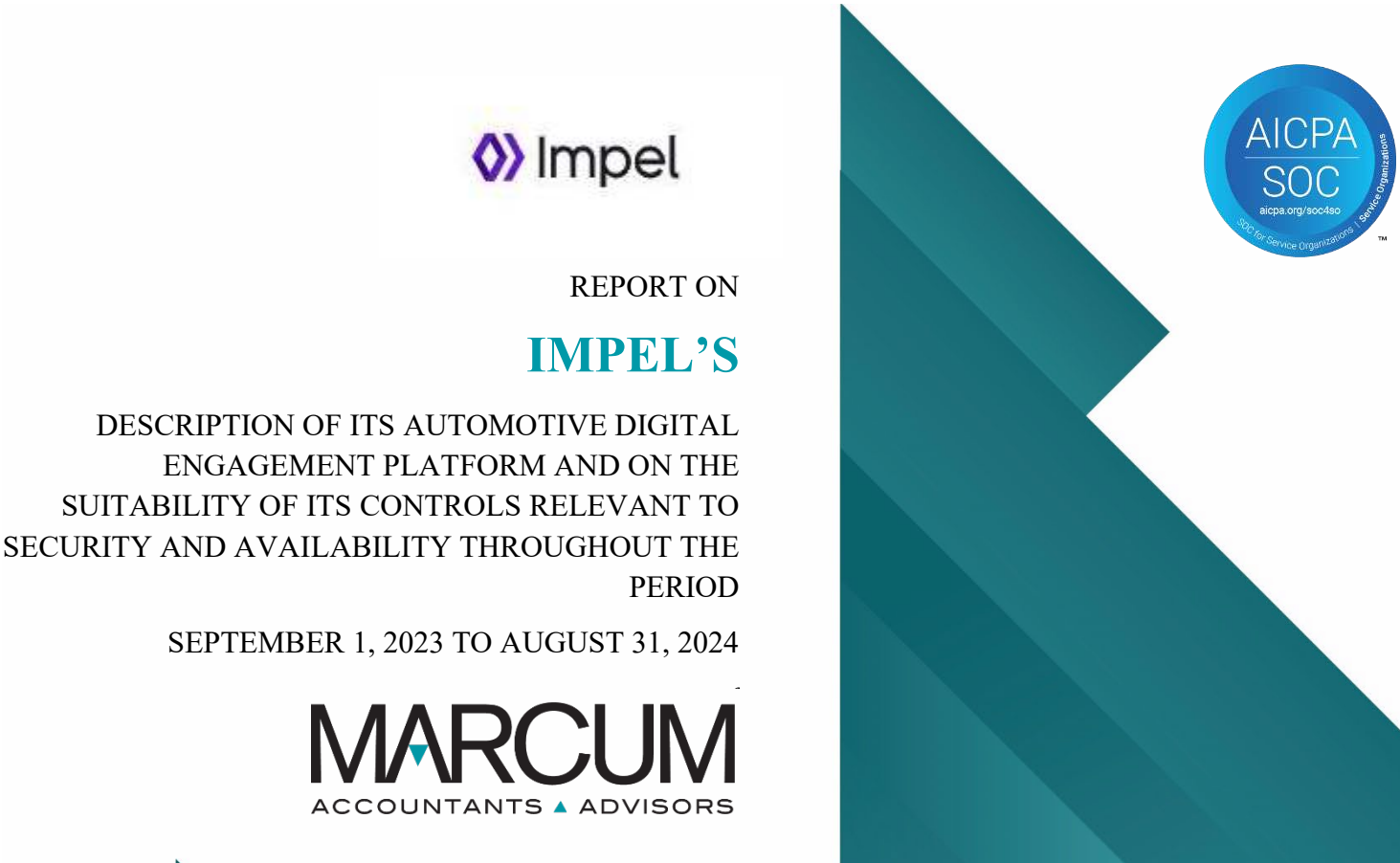

REPORT ON

IMPEL'S

DESCRIPTION OF ITS AUTOMOTIVE DIGITAL ENGAGEMENT PLATFORM AND ON THE SUITABILITY OF ITS CONTROLS RELEVANT TO SECURITY AND AVAILABILITY THROUGHOUT THE PERIOD

SEPTEMBER 1, 2023 TO AUGUST 31, 2024

MARCUM
ACCOUNTANTS ▲ ADVISORS

IMPEL– SOC 2 TYPE II TABLE OF CONTENTS

Acronym Table

AICPA	American Institute of Certified Public Accountants
AWS	Amazon Web Services
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CRM	Customer Relationship Management
CTO	Chief Technology Officer
DMS	Document Management System
IAM	Identity and Access Management
IT	Information Technology
MFA	Multi-Factor Authentication
RDS	Relational Database Service
SOC	Service Organization Controls
SSM	AWS System Manager
TSP	Trust Service Principles
VP	Vice President

Section 1: Assertion of the Management of Impel

Assertion of the Management of Impel

We are responsible for designing, implementing, operating, and maintaining effective controls within Impel's Automotive Digital Engagement Platform throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Impel's service commitments and system requirements were achieved based on the trust services criteria relevant to [Keywords] (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (*With Revised Points of Focus- 2022*), in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in attachment A and 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 September 1, 2023 to August 31, 2024, 2024 to provide reasonable assurance that Impel's service commitments and system requirements were achieved based on the applicable trust services criteria. Impel's 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 attachment B.

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 September 1, 2023 to August 31, 2024, to provide reasonable assurance that Impel's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Steven Saporta

CIO

Impel

October 30, 2024

Section 2: Independent Service Auditors' Report

MARCUM
ACCOUNTANTS ▲ ADVISORS

Independent Service Auditor's Report

To: Impel

Scope

We have examined Impel's accompanying assertion titled "Assertion of Impel Management" (assertion) that the controls within Impel's Automotive Digital Engagement Platform (system) were effective throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Impel's service commitments and system requirements were achieved based on the trust services criteria relevant to [Keywords] (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus- 2022)*, in AICPA Trust Services Criteria.

Service Organization's Responsibilities

Impel 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 Impel's service commitments and system requirements were achieved. Impel has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Impel 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 Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on 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 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 examination engagement.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Impel's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Impel's 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 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 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 Impel's Automotive Digital Engagement Platform were effective throughout the period September 1, 2023 to August 31, 2024, to provide reasonable assurance that Impel's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Marcum LLP

Marcum LLP

Tampa, FL

October 30, 2024

Attachment A: Impel ’s Description of the Boundaries of its Automotive Digital Engagement Platform

Company Overview and Services Provided

Augmented Reality Concepts, Inc., dba Impel is an end-to-end platform that combines the industry-leading conversational AI technology with best-of-breed applications for digital merchandising, communication and imaging. The platform was designed to help dealers get more from existing systems and processes. Impel's cloud-based technology seamlessly integrates with leading website platforms, third-party marketplaces, digital retailing tools, and DMS and CRM platforms to help deliver more engaging experiences.

Infrastructure

The key infrastructure supporting Impel's Automotive Digital Engagement Platform resides within AWS. Valid username and password combination plus MFA is required in order to authenticate into the AWS console. Impel has configured various IAM policies within the console that allow only certain users with certain policies attached to their IAM credentials to access various infrastructure components within the console. For instance, AWS SSM (policy) is only applied to the data science, engineering lead, and devops groups, which is the policy required in order to authenticate to EC2 instances. AWS security groups are in place to prevent unauthorized access to the instances. All data at rest (e.g. RDS volumes) and in motion are encrypted.

Software

The following provides a summary of the software and related services used in the delivery of the Automotive Digital Engagement Platform services:

- Bitlocker – utilized as the hard drive encryption software for company workstations.
- JIRA – utilized as the ticketing system for issue and project tracking.
- GitHub – utilized as a source code repository.
- BitBucket – also utilized as a source code repository.
- AWS CloudWatch – utilized as the monitoring and management service.
- AWS Inspector – utilized as a vulnerability scanning tool.
- AWS S3 – utilized for data storage.
- Crowdstrike – utilized as the antimalware solution on employee Windows workstations.

People

People involved in the operation and use of the system are:

- CEO, who is responsible for managing all day-to-day operations as well as long-term vision and strategy for the business, reporting the health of the business directly to the Board of Directors on an annual basis.
- CFO, who is responsible for overseeing management's ability to design, implement, and operate the organization's controls.
- CTO, who is responsible for the development, support, and security of the Automotive Digital Engagement Platform.

- VP, Customer Success, who is responsible for the onboarding of clients, support of clients, and fulfillment of operational processes and services to enable clients to realize the full value of the Automotive Digital Engagement Platform.
- IT Manager, who is responsible for the oversight of all corporate IT-related hardware, software, configuration, and security.

Processes and Procedures

Executive and operations management personnel maintain documented automated and manual standard procedures involved in the operation of Impel's Automotive Digital Engagement Platform that include:

- Access Control
- Change Management
- Data Backup Plan
- Device Management
- Incident Response Plan
- Information Security
- Personnel Security
- Risk Management
- Security Awareness Training

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently. Control procedures serve as mechanisms for managing the achievement of control activities and are a part of the process by which Impel strives to achieve its business objectives. Impel has applied a risk management approach to the organization in order to select and develop control procedures. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

The Impel control procedures that have been designed to meet the applicable trust services criteria are included in Section 4 of this report to eliminate the redundancy that would result from listing the procedures in this section as well.

Data

Data is a key component of Automotive Digital Engagement Platform. Data is obtained from Impel's clients (e.g. car dealerships) and imported into the system. To ensure the availability of the data, data is backed up in accordance with the data backup policy. AWS point-in-time recovery is enabled, with 30-day retention. While some data is purged after a set period or upon separation of a customer, other data is retained indefinitely.

System Boundaries

System boundaries, pertaining to collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third parties outside of the scope allowed in such contracts and agreements.

Risk Assessment

Impel's management performs an annual risk assessment, which requires management to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. Impel's management reevaluates the risk assessment annually or when otherwise necessary to both update the previous results and to identify new areas of concern.

Subservice Organization

Impel uses AWS for hosting production systems. AWS is responsible for the uptime, management, physical and logical security of the infrastructure that supports the delivery of internet, and environmental conditions that provide power and cooling to their devices. AWS is also responsible for providing physical security controls, administration of their hardware equipment, and reporting any logical or physical security incidents.

Communication

Internal Communications

Impel has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events were communicated. These methods include orientation for new employees and ongoing trainings for employees. Job descriptions are provided to employees and evaluations are completed against those job descriptions annually.

External Communications

Impel has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in communication of significant events. These methods include the use of e-mail messages and a customer contact option on the Impel website.

Attachment B: Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Impel designs its processes and procedures related to its Automotive Digital Engagement Platform to meet its objectives. Those objectives are based on the service commitments that Impel makes to user entities, the laws and regulations that govern service providers, and the financial, operational, and compliance requirements that Impel has established for the services.

Security

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Automotive Digital Engagement Platform that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect client data at rest and in transit.

Availability

Availability commitments to user entities are documented in customer agreements. Availability commitments are standardized and include, but are not limited to, the following:

- Managing capacity demand through the monitoring and evaluation of current processing capacity and usage rates.
- Meeting company objectives through authorization, design, development, and monitoring of data backup processes and recovery infrastructure.

MARCUMGROUP

Marcum Group is a family of organizations providing a comprehensive range of professional services including accounting and advisory, technology solutions, wealth management, and executive and professional recruiting.

These organizations include:

- Marcum LLP
  www.marcumllp.com
- Marcum Bernstein & Pinchuk
  www.marcumbp.com
- Marcum Insurance Services
  www.marcumis.com
- Marcum RBK Ireland
  www.marcumrbk.com
- Marcum Search
  www.marcumsearch.com
- Marcum Strategic Marketing
  marketing.marcumllp.com
- Marcum Technology
  www.marcumtechnology.com
- Marcum Wealth
  www.marcumwealth.com

MARCUM
ACCOUNTANTS ▲ ADVISORS

Ben Osbrach, CISSP, CISA, QSA, CICP, National Risk Advisory Leader
813.397.4860 ● ben.osbrach@marcumllp.com

Mark Agulnik, CPA, CISA, CIS LI, JD, Regional Advisory Partner-in-Charge
954.320.8013 ● mark.agulnik@marcumllp.com