FOUR51
STOREFRONT

APPLICATION ARCHITECTURE INFRASTRUCTURE & SECURITY

An in-depth look at the technology and procedures that power and manage the delivery of services from Four51

July 2021

INDEX

APPLICATION ARCHITECTURE

Four51's technical architecture is a private cloud model that leverages a combination of robust hardware, virtualization technology, and multiple data center facilities to deliver maximum application performance and reliability to our clients.

PLATFORM AS A SERVICE

UI	Responsive	JavaScript	HTML5	CSS3
APP	REST API		XML Web Service	
Service	Domain Business Objects			
Data	SQL Server			

Application Config
Admin Config
Catalog Config
Product Config
Supplier Config
Reporting
Integration

Delivered to the end user via a modern browser as a software as a service (SaaS) and a single page application, Four51 creates SAAS applications (such as Storefront, Approval, Employee Recognition, Corporate Identity and Proposal Generator) using the same REST API made available to customers. The REST API exposes the domain business objects for use in creating new applications or extending the publicly available source code of the applications created by Four51. The publicly available code repositories provided contain a full API coverage SDK, written with the Angular framework, to allow for rapid application development. These repositories are hosted on GitHub and can be quickly deployed and configured in the Four51 administration interface. All files in the source code can be easily edited, independent of the repository source, for additional customization.

Four51 maintains separate production, quality assurance, and test environments. All of the virtual and physical servers employed by the Four51 application run on Windows Server (2019, 2016 or 2012 R2) and are currently separated into front-end application servers and a back-end database server farm model.

The production IIS 8.5 and application servers are responsible for supporting user authentication, serving web page requests, hosting the Four51 interoperability web and XML services, and sending Four51 system messages. To increase availability, the production database server farm is running on Microsoft SQL 2014 Enterprise Edition and employing the native SQL 2014 Always On Availability Group cluster. In addition, Microsoft DFS (Distributed File System) is leveraged to create redundant file storage.

The Four51 application is also supported by a number of servers running specialized imaging applications (Pageflex Mpower). These imaging servers have been designed as a fault tolerant/load balancing solution and each server can be used to assume additional workload at any time should one of the other servers suffer a hardware failure or be taken down for maintenance.

INFRASTRUCTURE OVERVIEW

Four51 Infrastructure is partnered with OneNeck IT Solutions, and hosted on their Reliacloud service. Reliacloud is a private cloud model that provides the power and flexibility of a public cloud solution, with the security and performance required by enterprises with mission-critical computing needs. Built with industry-leading products and capabilities from Cisco, EMC and VMware, ReliaCloud is ideal for applications like Four51 that require reliable and scalable computing infrastructure.

ReliaCloud is delivered in dedicated and shared resource pools from multiple Tier III data centers and is architected for maximum flexibility and utilization of current IT investments with the ability to adjust as needs change.

Four51 has been Payment Card Industry (PCI) compliant since 2008 and SOC 2 Type 2 compliant since 2016. Four51 has consistently maintained an average 99.995% uptime over the last 10 years.

Four51 has implemented a disaster recovery plan using the services of OneNeck and Reliacloud. Their Hot DRaaS (Disaster Recovery as a Service) replicates the Four51 environment and creates near-complete backups of all critical data. In addition, a complete DR site is available should the DR response require it.

Each of these components play a critical role in ensuring that the Four51 application and our clients' data is secure, accessible and blazingly fast. Together with our key technology partners, Four51's infrastructure has been delivering comprehensive SaaS technology since 1999 to everyone from the smallest business to over half the Fortune 500.

INFRASTRUCTURE DIAGRAM

This section provides a detailed view of Four51's technology infrastructure and its three main components:

Data Center | Network/Routing | Servers

FOUR51 ELECTRONIC DATA PROCESSING DIAGRAM
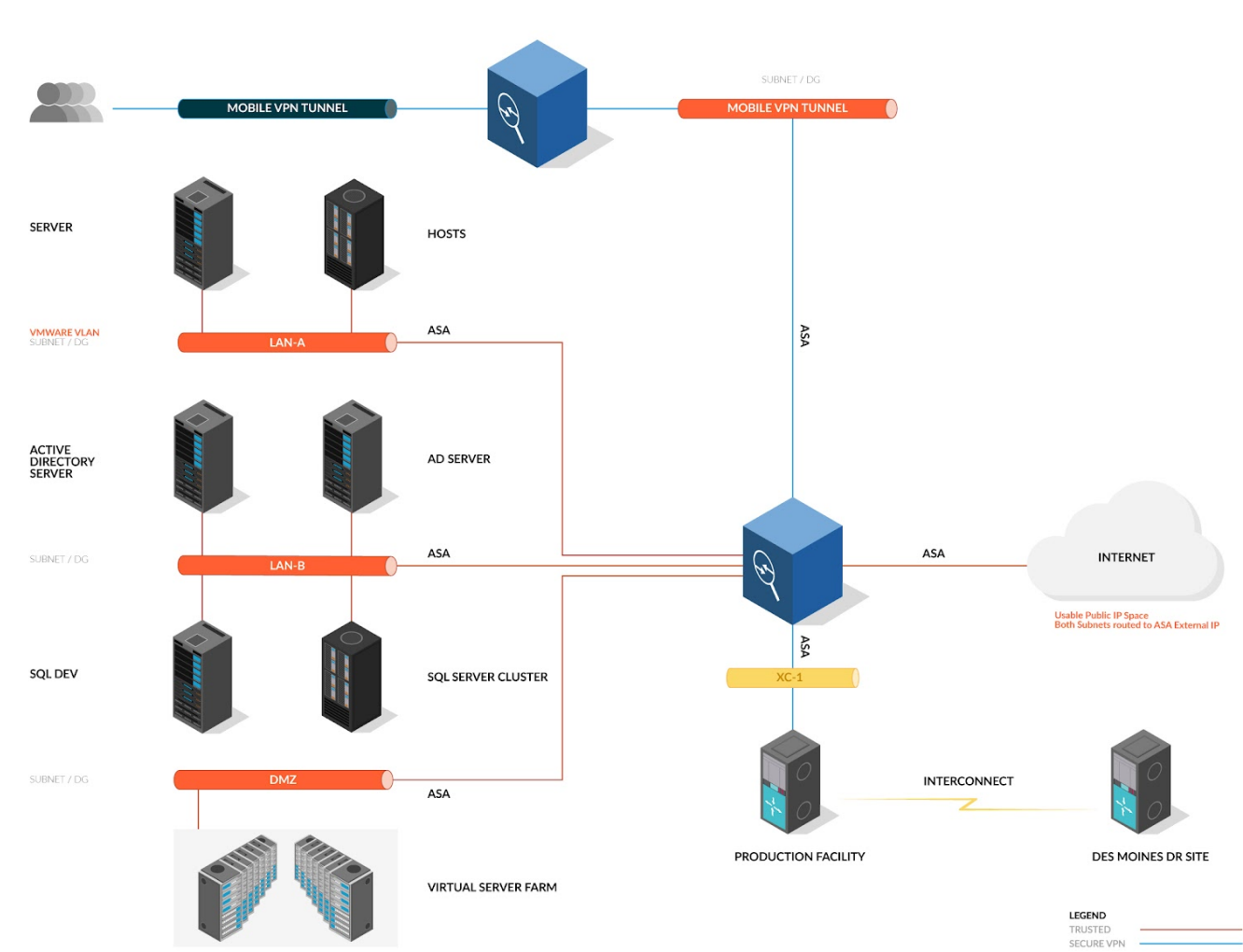
**NOTE: No portion of this network is wireless.

DATA CENTER

Four51 utilizes OneNeck Reliacloud, built upon a SSAE 16 (SOC 2) Type II certified and Uptime Institute Tier III design certified facility in Eden Prairie, MN (covers deprecated SAS 70 compliance). Features of the data center include exceptional security, redundant data and power connections, 24x7x365 support, extensive monitoring, intelligent climate control systems and cutting-edge suppression systems. This facility's internal control environment enables PCI, HIPAA, HITECH, SOX, and GLBA requirements.

What is Tier III Design Certification?

The Uptime Institute Tier Classification provides performance-based benchmarks to align business requirements with data center design. Tier III facilities offer uptime, thus availability assurance, to support the critical demands of production environments and critical applications.

The Data Center is designed to meet the demands of a concurrently maintainable infrastructure, with N+1 configured critical components deployed throughout the design. Currently connected to the N+1 degree to major Internet backbones through 3 different providers, this facility is provided with constant blistering high-speed access to and from the Internet. Organizations can rest assured that our facility provides the most redundant and available commercial data center environments in the United States.

What Makes Tier III Different?

The Tier III design employs a concurrently maintainable infrastructure. This assures that if any one critical data center component is removed through planned maintenance or component failure, service will not be interrupted.

Through the redundancy and concurrent maintainability in infrastructure, Tier III data centers provide the required availability and uptime to support mission-critical applications and 24x7x365 production environments. Tier III provides maximum uptime around:

- Power - both redundant utility feeds and quick-start Generac generators — ready to accept load from UPS in 5 seconds.
- Cooling - multiple independent cooling towers, independent environmentally controlled racks, equipment level cooling.
- Network - Carrier neutral facility serviced by 5 national backbone providers, independent network paths out of location in each direction (north, south, east, & west).
- Security - Triple authentication used: Key card, retina scan, and PIN to access facility. Trained guards, video surveillance, mantraps, biometric readers and location monitoring.

DATA CENTER SPECIFICATIONS

FACILITY

Design	Designed to Uptime Institute Tier III specifications.
Size	Design for over 18,000 usable square feet of raised floor
Access	24x7x365
Utility	Xcel Energy

CONNECTIVITY

Internet Bandwidth	Managed bandwidth and BGP routing across redundant Internet backbone connections with multiple Tier 1 carriers
Fiber	Redundant building fiber entrances
Type	Carrier neutral facility
Carrier	VISI/TDS, Qwest
Ports	Redundant bandwidth ports available

COOLING

Towers	N+1 evaporative cooling towers
Loops	Dual cooling loops
CRAC	N+1 30-ton CRAC units
PORTS	Water-side economizers

COMPLIANCE

Audit	SSAE 16 Type II
Security	Internal Control Environment enables PCI, HIPAA, SOX, and GLBA requirements

SUPPORT

Onsite Support	24x7x365 onsite technical support staff
Remote Hands	Remote hands and eyes support available
Managed Services	Monitoring, tracking, and reporting on alerts, incidents, and key event

SECURITY

Guard	Security guard present 24x7x365
Access Control	Three token authentication: Card access, biometric hand scan, and PIN
Surveillance	Video surveillance of data center and perimeter
Utility	Gaseous (under floor) and dry-pipe pre-action (overhead) fire suppression with VESDA early detection system

POWER

Pods	Three 1.29MW power pods
UPS	N+1 900kVA UPS systems
Generator	N+1 3.0MW Generators
Load	3.8MW total facility critical load

NETWORK ROUTING

Four51 subscribes to Cloud Committed and Cloud Burstable Internet Bandwidth to provide high performance, highly available Internet access. A multiple level firewall configuration with DMZ and secure data zones is used to maximize security. Only the Four51 application can access customer data. Servers containing customer data are behind a firewall and not accessible via the internet.

The Enterprise Firewall Service provides a dedicated security service instance that lives across highly available redundant hardware. The service includes security best practices, monitoring, and reporting of key metrics including port availability, interface utilization, and overall ASA/firewall health.

To moderate for legitimate Internet traffic, a robust anti-DDoS QoS policy is applied at the Internet edge, which sorts traffic into different policed classes that match on common signatures of DDoS traffic. In addition, an automated system is in place to watch for anomalous large volume traffic patterns. When this traffic crosses a threshold, the traffic for the attack target is automatically re-routed to a "choke" link, which constrains the traffic volume, and removes the traffic altogether from the data center's upstream Internet links.

SERVERS

The hosted private cloud architecture contains dedicated and hardened enterprise class host machines and associated hypervisor software (VMware ESX). Processors are provisioned with at least an aggregate 32 GHz per 256GB of RAM. Storage services (LUNs) are directly mapped via 8 GBPs fiber channel to the storage array. The LUN's are not shared or accessible by other Reliacloud customers. All arrays are D@RE enabled while the Nimble storage encrypts data at rest. All of the servers employed by the Four51 application run on Windows Server (2012 R2, 2016 or 2019), and are separated into front-end application servers and a back-end database server farm model.

The production application servers are responsible for supporting user authentication, serving web page requests, hosting the Four51 interoperability web and XML services, and sending Four51 system messages. The production database server farm is running on Enterprise Edition and employing the Always On Availability Group (AOAG) for failover and redundancy.

The Four51 application is also supported by a number of servers running specialized imaging applications (Pageflex Mpower). These imaging servers have been designed as a fault tolerant/load balancing solution and each server can be used to assume additional workload at any time should one of the other servers suffer a hardware failure or be taken down for maintenance.

With the hosted private cloud, Four51 achieves capacity expansion without the need for forklift upgrades, allowing the environment to scale with load and customer requirements. Roles and functions are not tied to specific machines, creating nearly infinite flexibility with capacity, speed, and redundancy. This standardized server platform also provides transparent server maintenance resulting in increased uptime and availability.

DISASTER RECOVERY

Great care and attention is given to ensuring that should the Four51 application lose functionality, data integrity, or uptime, all the appropriate resources and data can be restored quickly with as little downtime as possible.

The Four51 disaster recovery solution is comprised of two main facilities:

1. The primary hosted and private instance of the Reliacloud infrastructure is located in Eden Prairie, Minnesota. The environment is designed with sufficient infrastructure to withstand the loss of at least a single critical component. This is comprised of highly available virtual machines and dedicated servers running MS SQL Server Always On Availability Group (AOAG) to support Four51's primary database workload. If one server fails, the data goes live on the other. Similarly, application files are saved to a Distributed File System (DFS) Namespace which is immediately replicated to multiple file storage systems.
2. The secondary hosted private instance of Reliacloud is located in OneNeck's Des Moines, Iowa facility. This data center is comprised of another AOAG replica, and virtual machines running the same applications and utilities that are critical to operating the Four51 services.

Full backups of everything connected to the Four51 production environment, supporting servers and data, and Four51 resources are executed every week with incremental backups being executed every day. The Four51 archival policies call for a 35 day retention period on all mission-critical data points and customer data. After the retention period the expired data is removed and the free space rotated back into the recovery scheme for re-use.

In addition to AOAG, all Four51 application databases are fully backed up, with transaction log backups taken every 10 minutes. The backups are encrypted and stored so that archived data can be restored. Disaster recovery plans are tested monthly to assure that Four51 continues to operate at 99.99% scheduled uptime.

SECURITY

Four51 understands that security is mission critical and utilizes real time security monitoring from AT&T Cybersecurity. The Security Information and Event Management system (SIEM) provides real-time analysis of security alerts generated by applications and network hardware. The Four51 application, internal, and external infrastructure are regularly scanned for vulnerabilities.   All data is sent between a user's browser and the application over HTTPS and is secured with SSL certificates issued through DigiCert. Network participants' information is protected by undergoing a SOC 2 Type 2 audit, maintaining PCI compliance, maintaining CCPA & GDPR compliance, secure software and a secure application-hosting environment.

Four51 is PCI certified as a Level 2 Service Provider and adheres to the international payment card industry (PCI) compliance standards for data security. The payment card industry data security standards (PCI DSS) are network security and business practice guidelines adopted by Visa, MasterCard, American Express, Discover Card, and JCB to establish a "minimum security standard" to protect customers' payment card information.

Obtaining PCI certification means that Four51 has submitted for approval to a merchant bank our annual self-assessment questionnaire (SAQ D), a quarterly network scan from an approved scan vendor (ASV Coalfire), an annual penetration test (BreachLock) and an Attestation of Compliance. In addition, independent customer solicited security questionnaires and penetration tests have been performed verifying that the company

BUILDS AND MAINTAINS A SECURE NETWORK AND SYSTEMS
- Installs and maintains a firewall configuration to protect data
- Does not use vendor-supplied defaults for system passwords and other security parameters
- Regularly scans for network vulnerabilities

PROTECT CARDHOLDER DATA
- Protects stored data
- Encrypts transmission of cardholder data and sensitive information across public networks

MAINTAINS A VULNERABILITY MANAGEMENT PROGRAM
- Uses and regularly updates anti-virus software
- Develops and maintains secure systems and applications

IMPLEMENTS STRONG ACCESS CONTROL MEASURES
- Restricts access to data by business need-to-know
- Identifies and authenticates access to system components
- Restricts physical access to cardholder data

REGULARLY MONITORS AND TESTS NETWORKS
- Tracks and monitors all access to network resources and cardholder data
- Regularly tests security systems and processes
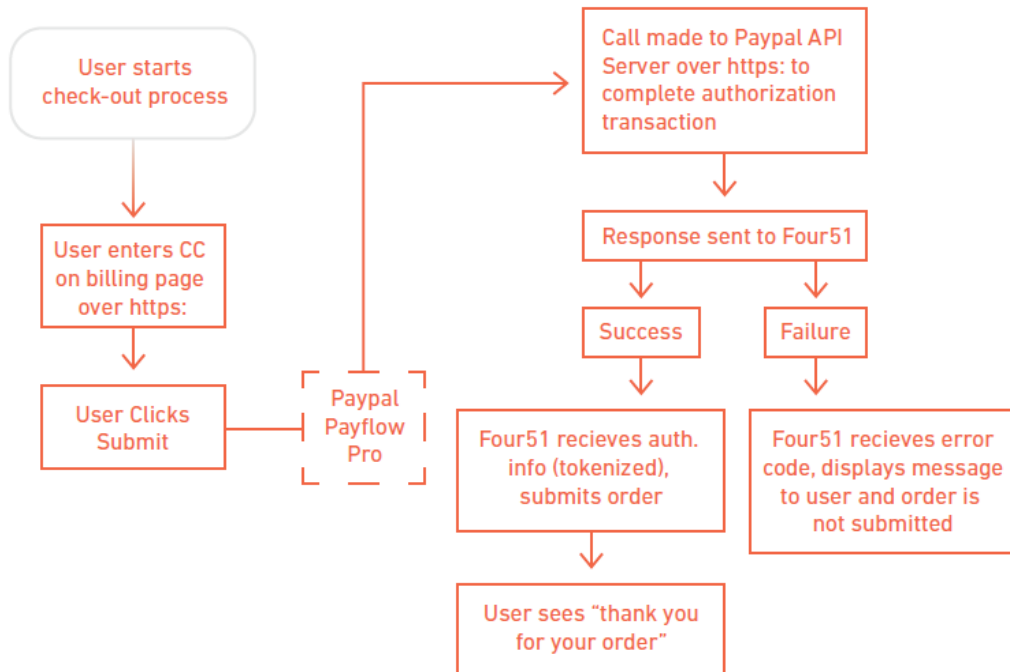
MAINTAINS AN INFORMATION SECURITY POLICY
- Maintains a policy that addresses information security

INFORMATION SECURITY POLICY

TABLE OF CONTENTS (Sample Only)

CREDIT CARD PROCESSING ON FOUR51

Payments by credit card are supported primarily by Four51 using Paypal technology. The flowchart above is an example of the creditcard flow and behaves the same for all credit card processing. When an order is placed with a credit card payment, the data is transmitted to Paypal for processing, and once authorized, the web server communicates with the database server to store non-sensitive and masked cardholder information along with the reference token. Because Four51 leverages reference transactions, the credit card number is not stored in the Four51 database. The credit cards are stored in memory until the order is submitted, and are never persisted or transmitted over a network.   Once the order is submitted, the buyer receives order confirmation details. Authorized users are then able to log in to the Four51 application via HTTPS and view order information, including the last four digits of the credit card number.

The following credit card processing mechanisms and endpoints are used:

PAYPAL PAY FLOW PRO

Four51 has developed this capability with the provided Payflow Pro SDK.
The endpoint is payflowpro.paypal.com.

PAYPAL PAYMENTS PRO

Four51 has developed this capability with the provided PayPal SDK. The endpoints used by this library are https://api.paypal.com/2.0/, and https://api-aa.paypal.com/2.0/

PAYCORP

Four51 has developed this capability with the provided Paycorp API. The endpoints used by this library are https://merchants.paycorp.com.au/paycentre/processEntry and https://merchants.paycorp.com.au/paycentre/makeEntry

IPSI

Four51 has developed this capability with the provided IPSI API. The endpoint used is
https://gateway.ipsi.com.au/v1.0

CardConnect
Four51 has developed this capability with the provided CardConnect API. The endpoint used is
https://fts.cardconnect.com:443/cardconnect/rest/

Transafe
Four51 has developed this capability with the provided Transafe API. The endpoint used is
https://live.transafe.com

PCI COMPLIANCE STATEMENT

Four51 is currently PCI DSS Level 2 compliant. Level 2 Compliance means that Four51 must annually submit to a qualifying merchant bank the following:

A SELF-ASSESSMENT QUESTIONNAIRE (SAQ-D)
The Four51 security team annually updates our Information Security Policy, performs an internal audit against the most recent PCI Data Security Standard and completes the self-assessment questionnaire (SAQ D). Four51's application is not eligible for validation under the Payment Application DSS (PA-DSS) because it is strictly a software as a service (SAAS) product and it is not sold, distributed, or licensed to third parties.

QUARTERLY NETWORK SCAN BY AN APPROVED SCAN VENDOR (ASV)
Four51 has leveraged a PCI ASV, Coalfire, and a web application scanning service from Rapid 7 to assist in monitoring and maintaining Level 2 compliance. The Coalfire service performs monthly scans against the Four51 network and the Rapid 7 service scans the application to ensure that the physical network and application are secure and in compliance. In addition to Four51 commissioned tests, customers have and are encouraged to perform their own security testing provided such tests are scheduled with the Four51 security team and are conducted during off-peak activity hours. The ASV scan report is found on page 24 of this document.

ATTESTATION OF COMPLIANCE FORM
The attestation of compliance is a signed document from a Four51 security officer stating that the company follows best security practices and is compliant with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures. Four51's Attestation of Compliance is included in this document on pages 13-23.

Additional documentation can be obtained from Four51 by an authorized security officer. If you have any other questions or concerns regarding PCI compliance, please have a member of your security team contact **info@four51.com**, or, if you are a Four51 customer, please submit a case.

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information			
Part 1a. Service Provider Organization Information			
Company Name:	Four51, Inc.	DBA (doing business as):	Four51, Inc.
Contact Name:	Jon Wylie	Title:	Chief Financial Officer
Telephone:	952.294.0451	E-mail:	jwylie@four51.com
Business Address:	110 North 5th Street, 3rd Floor	City:	Minneapolis
State/Province:	Minnesota	Country: United States	Zip: 55403
URL:	https:\\www.four51.io		
Part 1b. Qualified Security Assessor Company Information (if applicable)			
Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	Zip:
URL:			

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Four51 SAAS

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☒ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		

☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify):

Note: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed:	

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (specify):		

☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Four51 is a Software as a Service (SaaS) e-commerce platform located in Minneapolis, Minnesota that enables distributors (sellers) to provide a purchasing interface/shopping cart for their buyers. Via Four51, distributor's customers (buyer) place an order and the credit card authorization is handled by a third-party payment gateway (usually PayPal), or in the instance of qualified sellers Four51 passes the encrypted card number using private/public key in a cXML Order Request. No credit cards are processed or stored by Four51. Four51 does store the authorization code received from PayPal for transaction reference. The card number, card security code, or date of expiry are not stored.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Retail outlets	*3*	*Boston, MA, USA*
Four51 Corporate Office	1	Minneapolis,MN
OneNeck Reliacloud Hosting Facility	2	Eden Prairie, MN: Des Moines, IA (DR Site)

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes   ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment.

For example:
- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

The Four51 application is delivered to user's through a web browser over https. When an order is placed via the Four51 application with a credit card payment, the data is transmitted to the payment gateway over https for processing, and once authorized, the web server communicates with the database server to store non-sensitive and masked cardholder information along with the reference token. Four51 is a SOC 2 Type 2 certified service organization hosted in a private cloud. The server blades are D@RE enabled, and the Nimble Storage encrypts data at rest. Only the Four51 application can access customer data. Servers containing customer data are

	segmented from the network, behind two separate firewalls, and not accessible via the Internet.
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Part 2f. Third-Party Service Providers (Continued)

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of services provided:
OneNeck Reliacloud	Private Cloud Infrastructure, hosting and maintenance

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.

- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.

- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ

- Reason why sub-requirement(s) were not tested or not applicable

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:	Four51 SAAS

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	
Requirement 2:	☒	☐	☐	
Requirement 3:	☒	☐	☐	
Requirement 4:	☒	☐	☐	
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☒	☐	☐	
Requirement 9:	☒	☐	☐	
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☒	☐	☐	
Appendix A2:	☒	☐	☐	

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	October 5, 2020
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes ☒ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements in the SAQ identified as being not tested?	☐ Yes ☒ No
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated *October 5, 2020.*

Based on the results documented in the SAQ D noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (**check one**):

☒ | **Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Four51, Inc* has demonstrated full compliance with the PCI DSS.

☐ | **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provide Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*

☐ | **Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒ | PCI DSS Self-Assessment Questionnaire D, Version *3.2.1*, was completed according to the instructions therein.

☒ | All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.

☒ | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.

☒ | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.

☒ | If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

21

Part 3a. Acknowledgement of Status (continued)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Qualys*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **10/5/2020**
Service Provider Executive Officer Name: **Jon D. Wylie**	*Title:* **CFO**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	
Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	

---

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	**NO**	
1	Install and maintain a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.	☒	☐	

COALFIRE

Coalfire Systems, Inc. Scan Report – Attestation of Scan Compliance

Scan Customer Information		Approved Scanning Vendor Information	
Company: Four 51 - Storefront		**Company:** Coalfire Systems, Inc.	
Contact: Andy Mair	**Title:** Director, Infrastructure and Security	**Contact:** CoalfireOne Scanning Services	**Title:** CoalfireOne Scanning Services Manager
Telephone: 952.294.0451	**E-mail:** security@four51.com	**Telephone:** 650-597-4510	**E-mail:** cf1ss@coalfire.com
Business Address:	110 N 5th Street 3rd Floor	**Business Address:**	11000 Westmoor CIR STE 450
Country: United States	**City:** Minneapolis	**Country:** United States of America	**City:** Westminster
State/Province: Minnesota	**Zip:** 55403	**State/Province:** CO	**Zip:** 80021

Scan Status

- Compliance Status: Pass
- Number of unique components scanned: 3
- Number of active components: 3
- Number of identified failing vulnerabilities: 0
- Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 0
- Date scan completed: 2021-07-06T00:00Z
- Scan expiration date (90 days from date scan completed): 2021-10-04T00:00Z

Scan Customer Attestation

Four 51 attests on 07/06/2021 that this scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan disputes is accurate and complete. Four 51 also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

This scan and report was prepared and conducted by Coalfire Systems, Inc. under certificate number 5094-01-02, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. Coalfire Systems, Inc. attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by CoalfireOne Scanning Services.

INCIDENT RESPONSE PLAN

The Four51 incident response plan specifies a process for discovering, remediating and reporting incidents of application failure or a breach of security.

INCIDENT TYPES

Application service failures | Breach of personal information | Denial of service | Excessive port scans | Firewall breach | Misuse of service | System failures | Virus Outbreak | Storage Capacity | Unauthorized Wireless Access Point | System attach or compromise

INCIDENT DISCOVERY

- Monitor Four51 application and supporting services for log irregularities, performance and uptime
- Monitor Cisco, Open Web Application Security Project (OWASP) and Microsoft Technet advisories for software\hardware patches, security industry advisories and security alerts
- AT&T Cybersecurity monitors all server and IIS logs for irregularities and alerts staff to potential security issues
- Monitor physical access logs
- Schedule responsible personnel for incident response 24x7

SCHEDULED MAINTENANCE COMMUNICATIONS

Scheduled maintenance is a planned and deliberate event for the purpose of updating and/or performing maintenance to the Four51 application and/or hardware infrastructure. A regularly scheduled maintenance window is set for the first Sunday, following Microsoft's Patch Tuesday, between 11:00 pm – 2:00 am CST. "Patch Tuesday" occurs on the second, and sometimes fourth Tuesday of each month in North America. Additional maintenance may be necessary outside of this window, and whenever possible, will be scheduled after normal business hours typically between 11:00 pm and 5:00 am CST.

In the event of any scheduled maintenance, the following information will be posted for subscribers of status.four51.com: Date, time and expected duration of maintenance.

In the event of scheduled maintenance for the purposes of release notifications, the information is also posted to admin users within the application.

RECOVERY COMMUNICATIONS

In order to rapidly recover from potential unplanned system outages, the following procedures will be followed in the event of a system failure:

FOUR51 APPLICATION AND ADDITIONAL SERVICES INACCESSIBLE
- The Four51 technology team is notified via application monitoring utilities of the system failure
- The page at status.four51.com is updated
- Subscribers to the page at status.four51.com can choose whether to receive email or text alerts on status updates to specific Four51 application services.
- The service status is updated to eventually include start and end time of outage, duration, cause of failure, and any risk mitigation taken to prevent further outages.
- When possible, a splash page will be activated, indicating the application is unavailable, and, if known, time of restored services.

CONTACT

www.four51.com
info@four51.com
Twitter: @ordercloudio
LinkedIn: Four51, Inc
952-294-0451
110 N 5th St #300, Minneapolis, MN 55403