PCI DSS Scan Report Executive Summary

SYSNET GLOBAL SOLUTIONS
a VIKINGCLOUD® company
APPROVED SCANNING VENDOR

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	Clearcourse Events & Leisure Limited			Company:	Sysnet		
Contact:	Gary Riley	Title:		Contact:	Bob B.	Title:	ASV
Telephone:		Email:	gary.riley@clubsystems.com	Telephone:	+35314951300	Email:	support@sysnetgs.com
Business address:				Business address:	1st/3rd Floor Core A Block 71 The Plaza Park West Avenue Park West Business Park Dublin 12 Dublin, D12 Y4C0 Ireland		
URL:				URL:	https://www.vikingcloud.com/		
MID:	ClearCourseLeisure						

A.3 Scan status			
Date scan completed	July 23, 2026	Scan expiration date (90 days from date scan completed)	October 21, 2026
Compliance status:	PASS	Scan report type	Full Scan
Number of unique in-scope components[4] scanned			4
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

[4] A Components includes any host, virtual host, IP address, FQDN or unique vector into a system or cardholder data environment.

A.4 Scan Customer Attestation

Clearcourse Events & Leisure Limited attests on July 23, 2026 that this scan (either by itself or combined with multiple, partial or failed scans/rescans, as indicated in the above Section A.3 "Scan Status) 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 exceptions--including compensating controls if applicable--is accurate and complete. Clearcourse Events & Leisure Limited also acknowledges the following:

1. accurate and complete 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.

A.5 ASV Attestation

This scan and report was prepared and conducted by Sysnet under certificate number 509546-01-02, according to internal processes that meet PCI DSS requirement 11.3.2 and the ASV Program Guide. Sysnet 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, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Bob B.

ASV Scan Report Executive Summary

Part 1. Scan Information			
Scan Customer Company:	Clearcourse Events & Leisure Limited	ASV Company:	Sysnet
Date scan was completed:	July 23, 2026	Scan expiration date:	October 21, 2026

Part 2. Component Compliance Summary

IP Address: HTTPS://www.howdoipay.com:443/	PASS
IP Address: www.clubv1.com	PASS
IP Address: HTTPS://www.clubv1.com:443/	PASS
IP Address: www.howdoipay.com	PASS

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component[5]	Severity Level[6]	CVSS Score[7]	Compliance Status	Exceptions, False Positives, or Compensating Controls[8] (Noted by the ASV for this vulnerability)
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www. howdoipay.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
Consolidated Solution/Correction Plan for above Component					
ASV Comment:					
www.clubv1.com port 443/tcp	SLID-2010-0706 - Web Application Potentially Sensitive CGI Parameter Detection	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.

www.clubv1.com port 443/tcp	SLID-2018-0243 - jQuery Script Detection	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
www.clubv1.com port 443/tcp	SLID-2008-0160 - SSL Certificate Expiring Soon	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
www.clubv1.com port null/null	SLID-2011-0758 - Enumerated Hostnames	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
www.clubv1.com port null/null	SLID-2017-0052 - Operating System findings	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
Consolidated Solution/Correction Plan for above Component					
ASV Comment:					
HTTPS://www.clubv1.com:443/ port 443/https	SLID-2018-0355 - Full Path Disclosure	MED	6.5	PASS	This vulnerability is not recognized in the National Vulnerability Database.
HTTPS://www.clubv1.com:443/ port 443/https	SLID-2017-0655 - No Clickjacking Protection present	LOW	3.1	PASS	This vulnerability is not recognized in the National Vulnerability Database.
Consolidated Solution/Correction Plan for above Component					
ASV Comment:					
www.howdoipay.com port null/null	SLID-2011-0758 - Enumerated Hostnames	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
www.howdoipay.com port null/null	SLID-2017-0052 - Operating System findings	LOW	0.0	PASS	This vulnerability is not recognized in the National Vulnerability Database.
Consolidated Solution/Correction Plan for above Component					
ASV Comment:					

[5]Include CVE identifier and title and rank in descending order by CVSS score.
[6]High, Medium or Low Severity in accordance with Table 2 of the ASV Program Guide.
[7]Common vulnerability Scoring System (CVSS) base score, as indicated in the National Vulnerability Database (NVD), where available.
[8]Based on the information provided by scan customer, ASV agrees that the Compensating Control is relevant, applicable, and/or appropriate to address the vulnerability.

Part 3b. Special Notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
-	-	-	-

Part 3c. Special Notes - Full Text
Note

Part 4a. Scope Submitted by Scan Customer for Discovery
IP Addresses/ranges/subnets, domains, URLs, etc.
www.howdoipay.com
www.clubv1.com

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.
www.howdoipay.com
www.clubv1.com

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)
Requires description for each IP Address/range/subnet, domain, URL

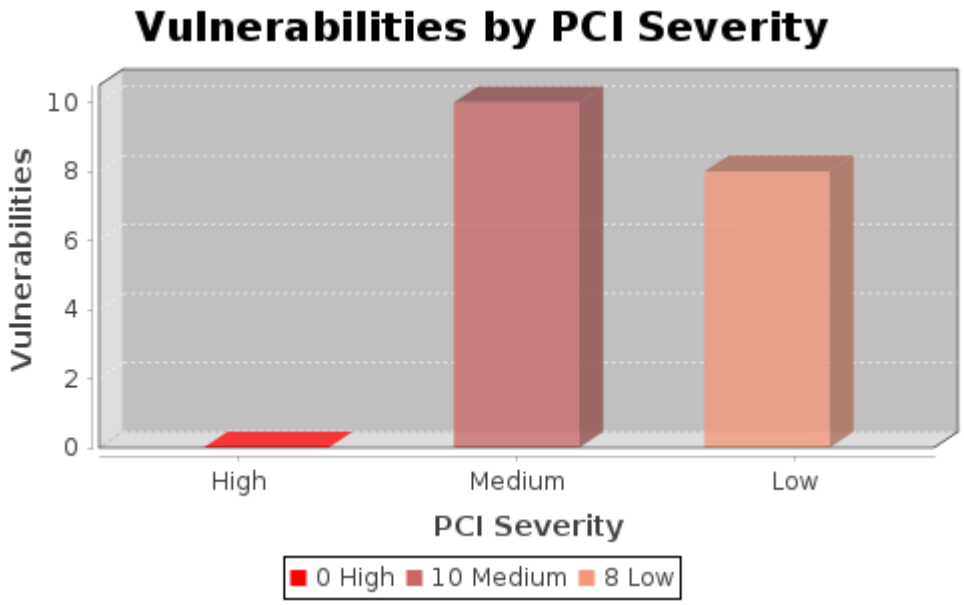
Summary of open TCP/UDP ports detected per component	
HTTPS://www.howdoipay.com:443/	TCP: UDP:
www.clubv1.com	TCP: 8172, 443 UDP:
HTTPS://www.clubv1.com:443/	TCP: UDP:
www.howdoipay.com	TCP: 8172 UDP:

Report Summary	
Company:	Clearcourse Events & Leisure Limited
Hosts in account	2
Hosts scanned	2
Hosts active	2
Scan date	July 23, 2026
Report date	July 23, 2026

Vulnerabilities by PCI Severity

Vulnerabilities total:	18

by PCI Severity	
PCI Severity	**Total**
High	0
Medium	10
Low	8
Total	18



Appendices

Hosts Scanned

HTTPS://www.howdoipay.com:443/, www.clubv1.com, HTTPS://www.clubv1.com:443/, www.howdoipay.com

Hosts Not Alive

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a useable format at https://www.pcisecuritystandards.org. Please send this completed form to PCI SSC at: asv@pcisecuritystandards.org.

ASV FEEDBACK FORM	
Client Name (merchant or service provider)	**Approved Scanning Vendor company (ASV)**
Name	Name
Contact	Contact
Telephone	Telephone
E-mail	E-mail
Business location where assessment took place	**ASV employee who performed assessment**
street	Name
city	Telephone
STATE/ZIP	E-mail
For each question, please indicate the response that best reflects your experience and provide comments. **4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree**	
1) During the initial engagement, did the ASV explain the objectives, timing, and review process, and address your questions and concerns?	
Response:	
Comments:	
2) Did the ASV employee(s) understand your business and technical environment, and the payment card industry?	

Response:
Comments:
3) Did the ASV employee(s) have sufficient security and technical skills to effectively perform this PCI Scanning Service?
Response:
Comments:
4) Did the ASV sufficiently understand the PCI Data Security Standard and the PCI Security Scanning Procedures?
Response:
Comments:
5) Did the ASV effectively minimize interruptions to operations and schedules?
Response:
Comments:
6) Did the ASV provide an accurate estimate for time and resources needed?
Response:
Comments:
7) Did the ASV provide an accurate estimate for scan report delivery?
Response:
Comments:
8) Did the ASV attempt to market products or services for your company to attain PCI compliance?
Response:
Comments:

9) Did the ASV imply that use of a specific brand of commercial product or service was necessary to achieve compliance?
Response:
Comments:
10) In situations where remediation was required, did the ASV present product and/or solution options that were not exclusive to their own product set?
Response:
Comments:
11) Did the ASV use secure transmission to send any confidential reports or data?
Response:
Comments:
12) Did the ASV demonstrate courtesy, professionalism, and a constructive and positive approach?
Response:
Comments:
13) Was there sufficient opportunity for you to provide explanations and responses during the scans?
Response:
Comments:
14) During the review wrap-up, did the ASV clearly communicate findings and expected next steps?
Response:
Comments:

15) Did the ASV provide sufficient follow-up to address false positives until eventual scan compliance was achieved?
Response:
Comments:
Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.

ASV FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS	
Name of ASV Client (merchant or service provider reviewed):	**ASV Company name:**
Payment Brand Reviewer:	ASV employee who performed assessment:
NAME	Name
TELEPHONE	Telephone
EMAIL	E-mail
For each question, please indicate the response that best reflects your experience and provide comments. **4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree**	
1) Does the ASV clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?	
Response:	
Comments:	
2) Did you receive any complaints about ASV activities related to this scan?	
Response:	
Comments:	
3) Did the ASV demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures?	
Response:	
Comments:	