

PCI DSS 6.4.3 AND 11.6.1 · WEEKLY REPORT

Script Inventory and Security Headers Report

Which vendors ran on Northwind Retail Group's payment pages, why each one is there, every script they served, and what changed in the security headers during the week.

VENDORS

17

SCRIPTS

30

APPROVED

13

REQUIRES ACTION

2

BLOCKED

2

HEADERS CHANGED

4

ORGANISATION

Northwind Retail Group

REPORTING PERIOD

21 to 27 September 2026

PAYMENT DOMAINS

checkout.northwind.com

pay.northwind.com

GENERATED

28 September 2026, 06:00 UTC

VENDORS AND SCRIPTS

17 vendors, 30 scripts.

Every vendor that ran on a payment page this week, the written justification for it, and each script it served. Vendors that need a decision come first.

Segment Analytics

Requires action
New this week

Awaiting review

JUSTIFICATION

No justification provided.

SUGGESTED Records checkout funnel events for conversion reporting. Reads click events and the email field.

SCRIPTS · 3

SCRIPT	SEEN ON	LAST SEEN
https://cdn.segment.com/analytics.js/v1/x/analytics.min.js SHA-256 3552ad5adad7efbc6cd7378638f5cd13e29061be5b3ac8ce53f4a659fc44ded5	pay	27 Sep
https://cdn.segment.com/analytics-next/bundles/ajs-destination.bundle.js SHA-256 987d2098451b63240756fef8bb1c5229460d5cbc781887b8ddf9dae513117e78	pay	27 Sep
https://cdn.segment.com/next-integrations/actions/amplitude-plugins/index.js SHA-256 f232066bb496cb5c691b0ae01c1f0152f06ec61f46c7a3f50adaced16b327fd2	pay	27 Sep

Chatly Support

Requires action

Awaiting review

JUSTIFICATION

No justification provided.

SUGGESTED Live support widget on the payment page. Reads keystrokes and the page URL.

SCRIPTS · 2

SCRIPT	SEEN ON	LAST SEEN
https://widget.chatly.com/loader.js SHA-256 ce31dc9555fe40772c7bf990272fbf75fc0a8e5935c29b8798203bbd9f240d88	checkout	27 Sep
https://widget.chatly.com/v2/widget.js SHA-256 241504346f7629dec39049f469b7a458c8545d96f6f0f4d0edc1c26050ee58e9	checkout	27 Sep

VENDORS AND SCRIPTS, CONTINUED

PartnerLoop Advertising

Blocked
[New this week](#)

Blocked by Dana Whitfield, 12 Sep 2026

JUSTIFICATION

Blocked on all payment pages. Unapproved ad pixel injected by container GTM-N7WQ2PX; no business owner identified.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://ads.partnerloop.net/conv.js SHA-256 b2000d6f6ccbbba63c9fe86e488d89be3e27c08fb7e9b99c5c18115461cab3b58	pay	25 Sep (blocked)

TagPilot Tag manager

Blocked
[New this week](#)

Blocked by Mika Rautio, 2 Sep 2026

JUSTIFICATION

Blocked on checkout.northwind.com. Reads card form fields.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://cdn.tagpilot.io/v3/pixel.min.js SHA-256 1d2e289e4758050d57a4e39dcb73e41a7f90eeb6a448e42ee91c2bb5362ce469	checkout	26 Sep (blocked)

Stripe Payments

Approved

Approved by Dana Whitfield, 4 Nov 2024

JUSTIFICATION

Tokenises card details in Stripe's iframe so the PAN never reaches our servers. Removing it stops card payments.

SCRIPTS · 4

SCRIPT	SEEN ON	LAST SEEN
https://js.stripe.com/v3/ SHA-256 15845cefb5695f6ec5de0a306ea37b8c16583835467b05390fd8781c116a6948	checkout, pay	27 Sep
https://js.stripe.com/v3/m-outer-3437aaddcdf6922d623e172c2d6f9278.html SHA-256 18fd822e4458dd2194d37c49abf273144a9b6320cd089702e71b8ab36b39418e	checkout, pay	27 Sep
https://js.stripe.com/v3/fingerprinted/js/elements-inner-card-8a2d4f1c.js SHA-256 91bcbcc665b6df94e236980e780b93f076c26de30445844aac2571c798d6734f	checkout, pay	27 Sep
https://m.stripe.network/out-4.5.44.js SHA-256 1777c744dcc4948855e498c5381c34d0cf0939f33b4621785667eddce354c7d4	checkout, pay	27 Sep

VENDORS AND SCRIPTS, CONTINUED

Script Monitoring Security ✓ Approved

Approved by Mika Rautio, 4 Nov 2024

JUSTIFICATION

Monitoring tag for PCI DSS 6.4.3 and 11.6.1. Inventories, verifies and can block every script on the payment pages.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://client.scriptmt.com/client.js SHA-256 809c9a4748f1f2a393817b4e3bf4b692699383785c95e4a2acbeb99c95c26439	checkout, pay	27 Sep

Cloudflare Security ✓ Approved

Approved by Mika Rautio, 18 Nov 2024

JUSTIFICATION

Turnstile bot challenge on the payment step, required by our card-testing fraud controls.

SCRIPTS · 3

SCRIPT	SEEN ON	LAST SEEN
https://challenges.cloudflare.com/turnstile/v0/api.js SHA-256 afc59ba23bd962db0b7f4c9888f9fe193e9210f4fbd4c0556e45fb3561b41dae	checkout, pay	27 Sep
https://challenges.cloudflare.com/turnstile/v0/g/b2f2c0c7/api.js SHA-256 411171db793004da5afcc9080608985ed2fb607f049e5face533d647b12e69cd	checkout, pay	27 Sep
https://static.cloudflareinsights.com/beacon.min.js SHA-256 2c032d7fba600c47f4cb5f0165f87e3103751e0c6a6d67cf84ca9c6d438b4ef7	checkout	27 Sep

AWS S3 CDN ✓ Approved

Approved by Mika Rautio, 4 Nov 2024

JUSTIFICATION

Serves our own checkout bundle from the northwind-static bucket.

SCRIPTS · 2

SCRIPT	SEEN ON	LAST SEEN
https://northwind-static.s3.eu-west-1.amazonaws.com/checkout/app.js SHA-256 c6c91e4c583ae8992b9ab072d58a727f7fa2619fe32149e13b2dd6a57c17fb97	checkout, pay	27 Sep
https://northwind-static.s3.eu-west-1.amazonaws.com/checkout/vendor.js SHA-256 482d591689c525a4c0e0a37bdd11ee74b06f980c1f2aa17768c84137a80930fc	checkout, pay	27 Sep

Amplitude Analytics ✓ Approved

Approved by Dana Whitfield, 9 Jan 2025

JUSTIFICATION

Behaviour analytics on the payment funnel: step views and drop-off. Configured not to read form field values.

SCRIPTS · 2

SCRIPT	SEEN ON	LAST SEEN
https://cdn.amplitude.com/libs/analytics-browser-2.11.0-min.js.gz SHA-256 06ddb4084d42adc31e7a3434e3bb88ab1c8e7fd0bc0924aff8166a6b43426bf1	checkout	27 Sep

VENDORS AND SCRIPTS, CONTINUED

Amplitude continued · script 2 of 2

SCRIPT	SEEN ON	LAST SEEN
https://cdn.amplitude.com/libs/plugin-ga-events-forwarder-browser-0.4.2-min.js.gz SHA-256 f804a5891a25aee10a49b24e3273de407852d74766d5793e80f3d800c59c710c	checkout	27 Sep

Google Analytics Analytics ✓ Approved

Approved by Joon-ho Park, 9 Jan 2025

JUSTIFICATION

Scripts support user interaction tracking and audience reporting.

SCRIPTS · 3

SCRIPT	SEEN ON	LAST SEEN
https://www.googletagmanager.com/gtag/js SHA-256 bdb62235ec2b69b78c95a39592a2d03fb885fbccf9faef477c818bda69b49e9f	checkout, pay	27 Sep
https://www.googletagmanager.com/gtag/destination SHA-256 7880fb934cb8abec4fc5c12f9773419726ec66d35bc622321cf93743454c2dde	checkout, pay	27 Sep
https://www.google-analytics.com/analytics.js SHA-256 f81d4c26afadd15dadbcd618376be2028d254ea7805155716a22cf2e1903f489	checkout	24 Sep

FullStory Session replay ✓ Approved

Approved by Dana Whitfield, 14 Apr 2025

JUSTIFICATION

Session replay for checkout usability. Card fields are excluded from capture by element-level masking.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://edge.fullstory.com/s/fs.js SHA-256 1dc2a465773f260d4a01d65e231d20fd4117cca1149c328bd85038022f98bada	checkout	24 Sep

Ahrefs Analytics ✓ Approved

Approved by Joon-ho Park, 3 Mar 2025

JUSTIFICATION

Scripts analyse user behaviour to improve checkout conversion reporting.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://analytics.ahrefs.com/analytics.js SHA-256 9715f3d9eba1a72dafa9c089943263edc00b77e5494657d05841ac1aa26c1dee	checkout	27 Sep

VENDORS AND SCRIPTS, CONTINUED

Google Ads Advertising ✔ Approved

Approved by Joon-ho Park, 2 Jun 2025

JUSTIFICATION

Scripts facilitate essential tracking for advertising conversion.

SCRIPTS · 2

SCRIPT	SEEN ON	LAST SEEN
https://googleads.g.doubleclick.net/pagead/viewthroughconversion/11506436942/ SHA-256 f6b91cd1f9a6bb4d81061b460cc30f688967b113182e7dc600e5047eaae36f49	checkout	27 Sep
https://www.googleadservices.com/pagead/conversion_async.js SHA-256 5c9dda67f10bd04a0e774004762a5b2cfe537c505c8cc1be173b608496a02de0	checkout	27 Sep

Criteo Advertising ✔ Approved

Approved by Joon-ho Park, 2 Jun 2025

JUSTIFICATION

Criteo's scripts are necessary for obtaining user conversion attribution.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://dynamic.criteo.com/js/ld/ld.js SHA-256 2eb36ada26bb6be3e0e074f24029116ae1f984e508b05f0f143d76e24b3392f3	checkout	22 Sep

Duration Media Advertising ✔ Approved

Approved by Joon-ho Park, 2 Jun 2025

JUSTIFICATION

The scripts support essential programmatic advertising placements.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://cdn.durationmedia.net/dm.js SHA-256 c5e489fa8134ca7b2eea0b9be82afd99178591a0874f596cadaaa9d6318f8dfe	checkout	24 Sep

AudienceLab (SuperPixel) Identity ✔ Approved

Approved by Joon-ho Park, 21 Jul 2025

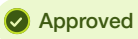
JUSTIFICATION

Scripts are utilised for tracking user interaction across paid campaigns.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://cdn.audiencelab.io/superpixel.js SHA-256 74a87b7398e6b653aa015a9a17ecfb76a61799a64dc9d5ac5c83a6a18bc801ed	checkout	24 Sep

VENDORS AND SCRIPTS, CONTINUED

G2 Other 

Approved by Joon-ho Park, 12 Aug 2025

JUSTIFICATION

Scripts for tracking clickthrough and conversion attribution from reviews.

SCRIPTS · 1

SCRIPT	SEEN ON	LAST SEEN
https://tracking-api.g2.com/attribution_tracking/conversions/1027539.js	checkout	27 Sep
SHA-256 277ba0b491eb8d64e8e765138494f7289b6da2d18c9be7a9bfa64aab66a715d1		

SECURITY HEADERS

All 14 security headers: 4 changed, 6 unchanged, 4 not set.

Every monitored header on the payment pages, as the consumer browser received it. Not set means the header was absent from every reading this week.

#	HEADER	VALUE THIS WEEK	STATUS
1	Content Security Policy	3 values this week. Before and after on pages 9 and 10.	● Changed
2	Content Security Policy Report Only	Not present	● Not set
3	Report To	{"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=nel-report-params"}]}	● Unchanged
4	Reporting Endpoints	2 values this week. Before and after on pages 9 and 10.	● Changed
5	Strict Transport Security	max-age=63072000; includeSubDomains; preload	● Unchanged
6	X-Frame-Options	DENY	● Unchanged
7	Cross-Origin Resource Policy	same-origin	● Unchanged
8	Cross-Origin Opener Policy	same-origin	● Unchanged
9	Cross-Origin Embedder Policy	Not present	● Not set
10	Permissions Policy	2 values this week. Before and after on pages 9 and 10.	● Changed
11	X-Content-Type-Options	nosniff	● Unchanged
12	X-Permitted-Cross-Domain-Policies	Not present	● Not set
13	Referrer Policy	2 values this week. Before and after on pages 9 and 10.	● Changed
14	X-XSS-Protection	Not present	● Not set

SECURITY HEADERS · CHANGED

What changed, with before and after.

Each value is shown in full once with its share of readings, then each change in order. Long values are laid out one directive per line, and their changes list only the directives that moved. Times are UTC.

Content Security Policy ● Changed 3 values

■	default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com	71.4%
■	default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com cdn.segment.com	26.9%
■	default-src 'self'; script-src 'self' js.stripe.com	1.7%

CHANGES · 3

Tue 22 Sep, 09:48 UTC · pay **cdn.segment.com added to script-src**

BEFORE default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com

AFTER default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com cdn.segment.com

Thu 24 Sep, 18:00 UTC · checkout **script-src narrowed during a deploy**

BEFORE default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com

AFTER default-src 'self'; script-src 'self' js.stripe.com

Thu 24 Sep, 18:35 UTC · checkout **Reverted**

BEFORE default-src 'self'; script-src 'self' js.stripe.com

AFTER default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com

Reporting Endpoints ● Changed 2 values

■	csp-endpoint="https://edge.scriptmt.com/csp"; max-age=10886400	99.6%
■	csp-endpoint="https://edge.scriptmt.com/csp"; max-age=5184000	0.4%

CHANGES · 2

Mon 21 Sep, 02:14 UTC · checkout **max-age shortened on one server**

BEFORE csp-endpoint="https://edge.scriptmt.com/csp"; max-age=10886400

AFTER csp-endpoint="https://edge.scriptmt.com/csp"; max-age=5184000

Mon 21 Sep, 02:40 UTC · checkout **Reverted**

BEFORE csp-endpoint="https://edge.scriptmt.com/csp"; max-age=5184000

AFTER csp-endpoint="https://edge.scriptmt.com/csp"; max-age=10886400

Permissions Policy ● Changed 2 values

■	camera=(), microphone=(), geolocation=()	98.2%
■	camera=(), microphone=(), geolocation=(), payment=(self)	1.8%

SECURITY HEADERS · CHANGED, CONTINUED

Permissions Policy ● Changed continued

CHANGES · 1

Fri 25 Sep, 13:20 UTC · pay **payment=(self)** added

BEFORE camera=(), microphone=(), geolocation=()

AFTER camera=(), microphone=(), geolocation=(), payment=(self)

Referrer Policy ● Changed 2 values

■ strict-origin-when-cross-origin	96.5%
■ no-referrer-when-downgrade	3.5%

CHANGES · 1

Wed 23 Sep, 11:05 UTC · checkout **Policy loosened on one edge node**

BEFORE strict-origin-when-cross-origin

AFTER no-referrer-when-downgrade

CHANGE LOG

Every change, in order.

WHEN (UTC)	WHAT CHANGED	DOMAIN	TYPE
Mon 21 Sep 02:14	Reporting Endpoints · max-age shortened on one server BEFORE csp-endpoint="https://edge.scriptmt.com/csp"; max-age=10886400 AFTER csp-endpoint="https://edge.scriptmt.com/csp"; max-age=5184000	checkout	● Header
Mon 21 Sep 02:40	Reporting Endpoints · Reverted BEFORE csp-endpoint="https://edge.scriptmt.com/csp"; max-age=5184000 AFTER csp-endpoint="https://edge.scriptmt.com/csp"; max-age=10886400	checkout	● Header
Tue 22 Sep 09:48	Content Security Policy · cdn.segment.com added to script-src BEFORE default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com AFTER default-src 'self'; script-src 'self' js.stripe.com challenges.cloudflare.com cdn.segment.com	pay	● Header
Tue 22 Sep 09:51	Scripts · Segment: 3 new scripts on a payment page AFTER https://cdn.segment.com/analytics.js/v1/x/analytic s.min.js https://cdn.segment.com/analytics-next/bundles/ajs-destination.bundle.js https://cdn.segment.com/next-integrations/actions/amplitude-plugins/index.js	pay	● Added
Wed 23 Sep 11:05	Referrer Policy · Policy loosened on one edge node BEFORE strict-origin-when-cross-origin AFTER no-referrer-when-downgrade	checkout	● Header
Wed 23 Sep 16:30	Scripts · Cloudflare Turnstile: new version BEFORE https://challenges.cloudflare.com/turnstile/v0/ap i.js SHA-256 eeb74aa08e0571b0b7c397d0811bb3ce4073ef138e09af29b7d9447e5f5a4881 24 KB AFTER https://challenges.cloudflare.com/turnstile/v0/g/b 2f2c0c7/api.js SHA-256 411171db793004da5afcc9080608985ed2fb607f049e5face533d647b12e69cd 51 KB, same origin	checkout, pay	● Changed

CHANGE LOG, CONTINUED

WHEN (UTC)	WHAT CHANGED	DOMAIN	TYPE
Thu 24 Sep 14:22	Scripts · Stripe tag: integrity attribute removed BEFORE https://js.stripe.com/v3/ integrity set on the <script> tag AFTER https://js.stripe.com/v3/ no integrity attribute	checkout	● Changed
Thu 24 Sep 18:00	Content Security Policy · script-src narrowed during a deploy BEFORE default-src 'self'; script-src 'self' js.stripe.co m challenges.cloudflare.com AFTER default-src 'self'; script-src 'self' js.stripe.co m	checkout	● Header
Thu 24 Sep 18:35	Content Security Policy · Reverted BEFORE default-src 'self'; script-src 'self' js.stripe.co m AFTER default-src 'self'; script-src 'self' js.stripe.co m challenges.cloudflare.com	checkout	● Header
Fri 25 Sep 10:05	Scripts · PartnerLoop attempted, blocked AFTER https://ads.partnerloop.net/conv.js SHA-256 b2000d6f6ccbba63c9fe86e488d89be3e27c08fb7e 9b99c5c18115461cab3b58	pay	✖ Blocked
Fri 25 Sep 13:20	Permissions Policy · payment=(self) added BEFORE camera=(), microphone=(), geolocation=() AFTER camera=(), microphone=(), geolocation=(), payment= (self)	pay	● Header
Fri 25 Sep 21:40	Scripts · Chatly loader: new hash, new outbound domain BEFORE https://widget.chatly.com/loader.js SHA-256 804ec97289980d99f1680dc8d4458005dc0c81c409 caf0963230461fb6ecfcee AFTER https://widget.chatly.com/loader.js SHA-256 ce31dc9555fe40772c7bf990272fbf75fc0a8e5935 c29b8798203bbd9f240d88 now sends keystroke data to a new domain	checkout	● Changed
Sat 26 Sep 03:12	Scripts · TagPilot attempted, blocked AFTER https://cdn.tagpilot.io/v3/pixel.min.js SHA-256 1d2e289e4758050d57a4e39dcb73e41a7f90eeb6a4 48e42ee91c2bb5362ce469	checkout	✖ Blocked