MEDIA INTERCEPT

GUIDE 09 / TRAFFIC QUALITY

THE NEWSLETTER ADVERTISER'S GUIDE TO INVALID TRAFFIC

How to identify, prevent, and manage low-quality clicks before they distort campaign performance.

Research edition Includes signal taxonomy, scanner logic, true-invalid vs suspicious rules, reason codes, review workflows, templates, checklists, and source notes.

How to use this guide

Invalid traffic is not a side issue in newsletter advertising. It affects advertiser confidence, publisher payouts, renewal decisions, and the credibility of the channel. This guide is designed to be used before, during, and after a campaign so teams can identify low-quality click activity without over-filtering legitimate readers.

The goal is not to label every unusual signal as fraud. The goal is to build a disciplined, evidence-based process that separates true invalid traffic, suspicious traffic, and non-payable traffic. Good review protects advertisers from inflated results and protects publishers from unsupported accusations.

Core premise	A valid newsletter click should represent a real reader intentionally engaging with an ad. A defensible traffic review explains why a click was kept, excluded, or moved to manual review.

This guide is written for four audiences:

- Advertisers and performance marketers who need confidence that they are paying for real engagement.
- Publisher monetization teams that want to protect earnings while responding fairly to traffic quality questions.
- Ad operations and analytics teams responsible for links, redirects, validation, exports, and reporting workflows.
- Finance and leadership teams deciding what gets paid, credited, held for review, or renewed.

The practical value is operational. The guide includes signal definitions, reason codes, review rules, workbook structures, advertiser and publisher templates, insertion order language, and checklists your team can turn into a standard operating process.

Table of contents

Content standard

This is an operating guide, not a blog post. A team should be able to use it to build a traffic-quality review process, explain payout adjustments, and prevent the same issues from repeating in the next campaign.

SECTION 01

EXECUTIVE SUMMARY

Invalid traffic is a measurement, trust, and payout problem - not just a technical issue.

1. Executive summary

Newsletter advertising works because it places brands inside trusted editorial environments. The value of that channel depends on the assumption that campaign metrics represent real reader engagement. Invalid traffic challenges that assumption. It can inflate clicks, depress apparent conversion quality, create gaps between platforms, and turn routine reporting into a payment dispute.

The first question should not be whether the publisher is wrong or whether the advertiser's analytics are wrong. The first question should be: what exactly was counted, at what point in the click path, and under what eligibility rules? A newsletter tracking platform may record a gross interaction. A validation provider may remove scanner or bot-like behavior. An affiliate system may count only accepted tracking endpoint loads. A site analytics platform may count only sessions after a page loads and scripts run. Those are different events.

Conclusion	Meaning	Action
Expected measurement gap	Systems count different events, but ratios are stable and explainable.	Document the expected range and keep optimizing.
Tracking setup issue	UTMs, click IDs, redirects, macros, landing scripts, or affiliate parameters failed.	Fix setup, annotate the report, and rerun QA.
Security-scanner inflation	Corporate or inbox security tools created non-human click-like events.	Filter using timing, user agent, IP/ASN, sequence, and validation logic.
Traffic quality issue	A material share of activity appears automated, duplicated, proxy-based, or otherwise unsupported.	Apply reason codes, exclude supported invalids, and preserve the audit trail.
Policy or eligibility gap	Traffic may be real but not payable under campaign terms, geography, date range, or advertiser rules.	Classify as non-payable rather than calling it fraud.

The mistake to avoid

Do not compare gross newsletter clicks to conversions and call the difference fraud. Reconcile the chain layer by layer: gross clicks to valid clicks, valid clicks to sessions or affiliate clicks, sessions to conversions, and conversions to approved or payable outcomes.

A useful traffic-quality report does three things. It explains the difference between data sources, separates setup problems from traffic-quality problems, and states which clicks are payable, excluded, or unresolved. It should not simply say that the numbers do not match.

What the final answer should include

- The gross click count, the valid click count, the excluded click count, and the unresolved count.
- The reason-code breakdown for excluded clicks, including duplicate, bot, scanner, data center, proxy/VPN, geo, and policy-based removals.
- The largest drop-off layer, such as gross-to-valid, valid-to-affiliate, affiliate-to-session, or session-to-conversion.
- A clear decision on what is billable, payable, credited, held for review, or changed before the next send.

SECTION 02

WHAT COUNTS AS INVALID TRAFFIC

A valid click should reflect reader intent. Invalid traffic should be excluded only when the evidence supports it.

2. What invalid traffic means in newsletter advertising

Invalid traffic is traffic that should not be counted as a legitimate advertising interaction. In newsletter advertising, the most common unit is the click. That click may influence performance analysis, advertiser billing, publisher payout, renewal decisions, or makegood decisions. Because money and trust can depend on the number, the definition matters.

A valid click should represent a human reader intentionally engaging with a newsletter ad, sponsorship, dedicated email, text link, or offer. An invalid click may come from automated systems, duplicated events, crawlers, server-side tools, security scanners, non-browser user agents, or other sources that do not represent real reader intent.

Figure: a click is not one event

Each system counts a different event. Reconcile adjacent layers instead of comparing one top-line number to another.

Invalid traffic in newsletters is different from invalid traffic in display advertising because email sits between several systems: the publisher's email service provider, tracking platform, advertiser analytics, affiliate or attribution platform, inbox protection tools, link wrappers, redirects, and reader privacy tools. Each system can touch the link before or after the human reader does.

Traffic type	What it means	Recommended treatment
Valid click	Unique, human-initiated, inside campaign rules, not filtered by quality rules.	Keep as payable or reportable.
Invalid click	Strong evidence of non-human, duplicate, blocked, crawler, or automated activity.	Exclude with a reason code.
Suspicious click	Risk signal exists, but it is not strong enough by itself to prove invalid activity.	Move to review or combine with other signals.
Non-payable click	May be real, but does not qualify under IO, advertiser rules, geography, date range, or payment policy.	Exclude from payout but avoid fraud language.

Working definition

A click should be excluded only when it is clearly invalid, clearly outside campaign terms, or clearly unsupported by the agreed validation policy. Anything else belongs in a manual review bucket.

Why this distinction protects both sides

Advertisers need to avoid paying for inflated or non-human activity. Publishers need to avoid having valid audience engagement discounted by vague accusations. The best language is precise: invalid, suspicious, non-payable, unresolved, or payable. Each term should mean something specific.

SECTION 03

THE NEWSLETTER MEASUREMENT CHAIN

Most discrepancies become understandable when every team knows where each platform counts.

3. The newsletter measurement chain

A newsletter click does not travel directly from reader to conversion. It passes through a sequence of systems. At each stage, a platform decides whether it saw an event, whether it can associate the event with the campaign, and whether the event qualifies for reporting, billing, attribution, or payout.

Stage	What happens	Common count
1. Email delivered	Message is sent and may be scanned, filtered, or link-rewritten before the recipient sees it.	Delivered, opened, scanned
2. Link interaction	A reader or scanner touches the tracked link. The newsletter platform may count this event.	Gross click
3. Tracking redirect	Tracking domain records timestamp, placement, publisher, subscriber or hashed identifier, and destination.	Newsletter click
4. Validation review	Rules flag duplicates, bot user agents, scanner patterns, data center traffic, proxies, or geo issues.	Valid or invalid click
5. Affiliate or advertiser endpoint	Affiliate network or advertiser tracking accepts parameters, click IDs, and sub IDs.	Accepted click
6. Landing page load	User reaches the site. Analytics counts a session if the page loads and tracking is allowed.	Session, user, pageview
7. Conversion and approval	Lead, purchase, signup, or event fires and may be approved, rejected, reversed, or unattributed.	Conversion, approved event

Why one-to-one comparisons break

A newsletter gross click and an analytics session are related metrics, but they are not interchangeable. A gross click can include scanners, duplicate activity, or a user who closes the tab before the page loads. A session can be lost because JavaScript was blocked, consent was denied, the page was slow, or the tracking parameter was stripped. Affiliate clicks can be lower if the required network parameters did not load or if the network filtered the click.

Operational rule

Every report should label the metric by where it was measured: gross newsletter click, validated click, affiliate click, landing session, conversion event, approved conversion, or payable click.

Example layer view

Layer	Count	Rate vs previous layer	Diagnostic meaning
Gross newsletter clicks	10,000	Baseline	Top-level interaction before quality review.
Validated clicks	8,150	81.5%	18.5% removed by scanner, duplicate, bot, or eligibility rules.
Affiliate clicks	7,620	93.5%	Most validated clicks reached the affiliate endpoint.
Landing sessions	6,810	89.4%	Some loss from page load, consent, ad blockers, or analytics definitions.
Conversions	420	6.2% of sessions	Downstream engagement after landing.
Approved conversions	356	84.8%	Final payout or approval layer.

SECTION 04

WHY INVALID TRAFFIC HAPPENS

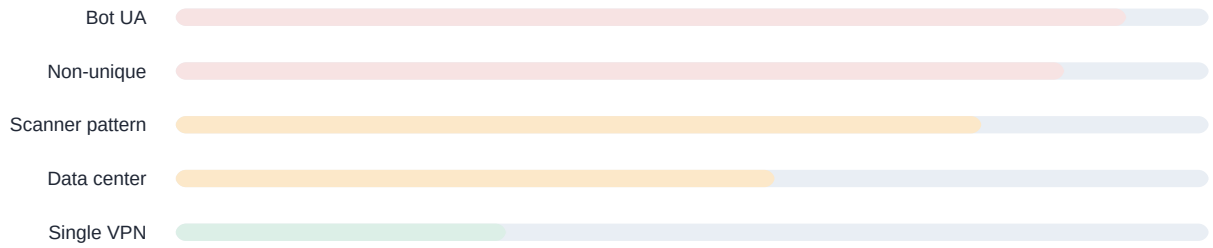
Not all invalid traffic is malicious. Some is caused by legitimate systems that protect inboxes.

4. Why invalid traffic happens

Invalid traffic does not always mean a publisher intentionally did something wrong. Some invalid clicks come from legitimate security systems, link-checking tools, corporate gateways, crawlers, privacy tools, or duplicate events. Some comes from low-quality or abusive sources. A strong process can tell the difference without overreaching.

Cause	What it looks like	What to check first
Email security scanner	Clicks immediately after send, sometimes across multiple links, often no downstream session.	Time-to-click, link sequence, user agent, IP/ASN, recipient domain.
Crawler or bot	Known bot user agent, non-browser client, repeated automated patterns.	User agent strings, validation status, IP source, behavior pattern.
Duplicate activity	Same source repeats within a short window or platform marks non-unique.	Click ID, hashed recipient, IP, device, timestamp window.
Data center or hosting network	Traffic comes from cloud or server infrastructure instead of ordinary access networks.	ASN, organization, user agent, session behavior, repeat patterns.
Proxy or VPN	Location and identity may be masked. Some traffic may be real but harder to verify.	Overlap with data center, repeats, bot UA, geo rules, advertiser exclusions.
Geo or targeting mismatch	Traffic outside approved markets, languages, devices, or audience rules.	IO terms, campaign brief, country, device, offer eligibility.
Intentional manipulation	Unnatural spikes, repeated sources, low engagement, suspicious publisher concentration.	Multi-signal evidence, historical baselines, validation provider findings.

Evidence strength by signal type



Treat signals as evidence, not labels. A single soft signal should usually move to review, not automatic removal.

The evidence standard

The more serious the conclusion, the stronger the evidence should be. A single VPN flag is not the same as a bot user agent. A single repeat IP is not the same as hundreds of clicks from one hosting ASN within minutes. The review process should grade signals by strength and require multiple signals for softer categories.

Language standard

Use neutral language until the evidence is clear. 'Non-human activity', 'scanner-like pattern', 'non-payable traffic', and 'unsupported click activity' are usually more accurate than 'fraud' during the review stage.

SECTION 05

INVALID VS SUSPICIOUS VS NON-PAYABLE

A precise classification framework prevents confusion and protects the relationship.

5. Invalid, suspicious, and non-payable traffic

One of the biggest mistakes in traffic review is treating every questionable signal the same way. Not every suspicious click is invalid. Not every non-payable click is fraudulent. Not every proxy, VPN, repeat IP, or corporate network means a publisher acted improperly. A better framework separates the traffic into three categories.

Category	Definition	Examples	Decision
True invalid	Strong evidence that the click does not represent legitimate human engagement.	Bot/crawler user agent, platform non-unique, blocked status, rapid duplicate, known automated scanner.	Remove and record reason code.
Suspicious	Risk signals exist, but the signal alone is not enough to prove invalid activity.	Single VPN flag, cloud ISP, corporate network, unusual browser, repeat IP without extreme volume.	Review, combine with other signals, or keep.
Non-payable	Traffic may be real but does not qualify under campaign terms or advertiser rules.	Outside geography, outside date range, excluded placement, advertiser-specific exclusion, unpaid advertiser campaign.	Exclude from payout under policy, not fraud language.

Why it matters

The final report should not just state how many clicks were removed. It should say why they were removed and whether they were invalid, suspicious but unresolved, or non-payable under the agreed terms.

Category examples

A click from a bot user agent can often be excluded automatically. A click from a VPN should usually be reviewed in context. A non-US click on a US-only campaign may be non-payable even if it came from a real person. A click tied to an advertiser that will not pay may be a finance or contract issue, not a traffic-quality issue.

What to say to partners

- For true invalid traffic: 'These clicks were excluded because they matched our documented invalid traffic rules.'
- For suspicious traffic: 'These clicks were reviewed because they had risk signals, but we only excluded records with additional supporting evidence.'
- For non-payable traffic: 'These clicks were removed from payable totals because they do not qualify under the campaign terms, not because we are alleging publisher misconduct.'

SECTION 06

SIGNAL TAXONOMY

Reason codes turn vague concerns into a repeatable review process.

6. The invalid traffic signal taxonomy

A traffic-quality process should use the same reason codes every time. Vague categories like 'bad traffic' or 'tracking issue' create confusion and make the review difficult to defend. Reason codes should point to evidence and to the right next action.

Code	Reason	Definition	Default treatment
NON_UNIQUE	Platform non-unique	Platform identifies the click as a duplicate or repeat event.	Remove.
BOT_UA	Bot/crawler user agent	User agent identifies a crawler, bot, script, monitor, or automated client.	Remove.
NON_BROWSER	Non-browser client	Click does not come from a recognizable browser or app environment.	Remove when clear; otherwise review.
SCAN_FAST	Immediate scanner pattern	Click occurs within a fast-click window and matches scanner indicators.	Remove if supported by sequence or source.
SCAN_MULTI	Multi-link scanner	Multiple links from the same recipient/IP/UA fire in rapid sequence.	Remove affected automated activity.
DUP_WINDOW	Duplicate within window	Repeated click from same entity inside defined dedupe window.	Keep first valid click, remove duplicates.
DC_ASN	Data center or hosting ASN	IP/ASN associated with cloud, hosting, or automated infrastructure.	Review; remove with other signals or policy.
PROXY_VPN	Proxy or VPN	Traffic appears masked or routed through proxy/VPN infrastructure.	Review; remove with other signals or policy.
GEO_OUT	Ineligible geography	Traffic is outside agreed campaign geography.	Non-payable if terms require.
TEST_INTERNAL	Proof or internal traffic	Known QA, internal, seed-list, or proofing activity.	Remove from final performance.
BROKEN_PATH	Tracking path failed	Newsletter click did not correctly reach affiliate or landing path due to setup issue.	Exclude or credit depending on fault.
UNRESOLVED	Insufficient evidence	Flagged for review but not enough support for exclusion.	Hold for review or keep separately.

How to choose a reason code

Assign the most specific code supported by the data. If a click is a bot user agent and a duplicate, the bot user agent code is often the stronger reason. If a click is only a proxy flag with no other anomaly, it may belong in PROXY_VPN review rather than automatic removal. If a click is outside the approved geography, it may be GEO_OUT even if it was human.

Auditability rule

Every excluded click needs a reason code. Every reason code needs a written definition. Every final report should separate excluded, unresolved, and payable clicks.

SECTION 07

SECURITY SCANNERS AND BOT CLICKS

Security tools can create click-like events without reader intent.

7. Security scanners and bot clicks

Email security systems often inspect, rewrite, or verify URLs to protect recipients from phishing and malware. This is legitimate security behavior, but it can complicate ad measurement because the security system may interact with links before or around the time a human reader does.

Scanner behavior is especially common in B2B, finance, healthcare, enterprise, and professional audiences where corporate inbox protection is common. These clicks can inflate gross click totals while producing little or no downstream session depth, affiliate activity, or conversion behavior.

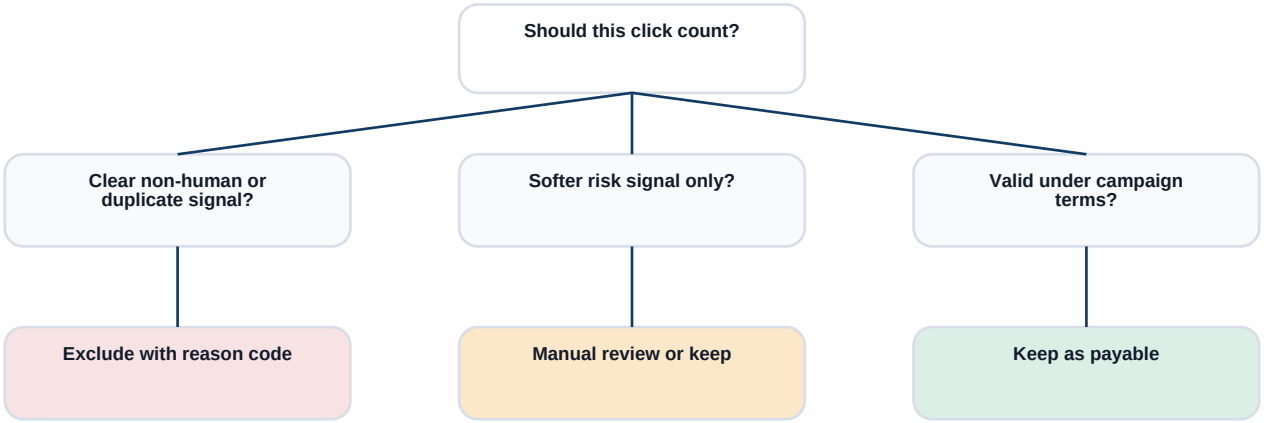
Scanner signal	Why it matters	What to check
Very fast time-to-click	A large cluster seconds after delivery is unlikely to be normal human reading behavior.	Send timestamp, click timestamp, fast-click threshold.
All-link or multi-link sequence	Scanners often inspect every link or multiple links in a message.	Link sequence, recipient/hash, IP, user agent.
No landing engagement	Scanner may not load the destination like a normal browser session.	Affiliate clicks, GA4 sessions, server logs, events.
Security-provider network	Some scans originate from identifiable security or corporate infrastructure.	IP organization, ASN, hostname, domain.
Repeated user agent	Automated systems may use repeated or incomplete user agents.	UA string, browser family, device, JavaScript capability.
First-link bias	Some systems inspect the first or every visible link in the HTML.	HTML link order and affected URLs.

Important distinction

A scanner click is not the same as malicious fraud. It is non-human and should not be treated as qualified reader traffic, but it may be caused by legitimate enterprise security software rather than intentional inflation.

Scanner mitigation options

- Capture raw timestamp, IP or hashed IP, ASN, user agent, recipient domain, link ID, and publisher where privacy rules allow.
- Flag immediate multi-link activity from the same source instead of excluding all fast clicks blindly.
- Separate gross clicks from eligible or validated clicks in every report.
- Use manual review for ambiguous scanner-like activity.
- Explain scanner filtering in advertiser reports so buyers understand why valid clicks can be lower than gross clicks.



Decision rule: exclude only when evidence, policy, and documentation support the removal.

SECTION 08

PROXY, VPN, AND DATA CENTER TRAFFIC

Network signals are useful, but they should not be treated as proof by themselves.

8. Proxy, VPN, and data center traffic

Proxy, VPN, and data center signals are common sources of confusion. They can indicate masked, automated, or low-quality traffic. They can also represent legitimate users browsing through work networks, privacy tools, mobile infrastructure, travel environments, or corporate security systems. The signal is meaningful, but it is not always definitive.

Signal	What it may mean	When it becomes stronger	Default treatment
Single VPN flag	A user is routing through a VPN for privacy, travel, security, or work.	Combined with repeats, data center ASN, no sessions, or geo mismatch.	Review only.
Proxy flag	Traffic may be masked or routed through an intermediary.	Combined with high frequency, non-browser UA, or campaign ineligible geography.	Review or exclude by policy.
Data center ASN	Traffic originates from hosting or cloud infrastructure.	Combined with automation, repeated timestamps, bot UA, or no downstream activity.	Review, then exclude if supported.
Corporate network	Normal business users or enterprise security infrastructure.	Fast multi-link patterns or no human landing behavior.	Review in context.
Mobile carrier proxy	Carrier routing may distort IP and location.	Paired with abnormal repetition or ineligible market.	Usually keep unless policy says otherwise.

The overlap rule

A proxy flag alone should usually not be enough to remove a click under a true-invalid-only policy. Proxy plus data center plus rapid repeat activity is a much stronger removal case. VPN plus normal browser plus normal time distribution may be a valid reader. Data center plus bot user agent is likely non-human. The point is to evaluate the pattern, not the label.

Policy option

Advertisers can define proxy, VPN, or data-center traffic as non-payable in advance. If that is the rule, document it in the insertion order or campaign terms so publishers are not surprised after delivery.

Questions to ask before excluding network-signal traffic

- Is the campaign geo-restricted or audience-restricted?
- Is the signal isolated or paired with another anomaly?
- Does the click have downstream engagement such as sessions, page depth, or conversion behavior?
- Does the pattern concentrate by one publisher, one IP/ASN, one device, or one timestamp window?
- Did the advertiser define this source as non-payable before the campaign?

SECTION 09

DUPLICATE AND RAPID REPEAT ACTIVITY

Duplicate rules should preserve legitimate first clicks while excluding inflated repeat events.

9. Duplicate and rapid repeat activity

Duplicate clicks are not always invalid. A real reader can click the same link twice, refresh a page, return later, or click from multiple devices. The problem is when repeated activity is so close, frequent, or patterned that it no longer looks like normal engagement.

Duplicate pattern	Possible cause	Recommended handling
Same user/hash clicks same link within seconds	Double click, scanner, duplicate firing, accidental repeat.	Keep first valid click; remove rapid repeats.
Same IP clicks many times across one campaign	Shared office, scanner, bot, proxy, or manipulation.	Review volume, UA, timing, and sessions.
Same user clicks multiple different links at same timestamp	Security scanner or link checker.	Exclude scanner-like sequence with reason code.
Same user returns hours later	Legitimate revisit or comparison shopping.	Usually keep unless outside defined unique window.
Platform marks click as non-unique	Platform dedupe already recognized repeat activity.	Remove or report separately from unique clicks.

Recommended dedupe hierarchy

- Use the strongest available identifier first: click ID, subscriber hash, user ID, or platform unique key.
- Where identifiers are unavailable, use a conservative combination of IP or hashed IP, user agent, placement, link ID, and timestamp.
- Define a rapid duplicate window, such as seconds or minutes, and document it before final reconciliation.
- Keep the first valid click when appropriate and exclude only the repeated events.
- Separate platform non-unique clicks from manual duplicate rules so the audit trail remains clear.

Avoid over-filtering

A duplicate rule should not remove every repeat visitor. It should remove activity that is inconsistent with human intent or outside the agreed unique-click definition.

Example duplicate policy

For CPC campaigns, the team may define payable clicks as unique, human-initiated clicks after validation. Under that policy, repeated clicks from the same click ID, subscriber hash, or source inside a defined rapid window can be excluded as DUP_WINDOW. Longer-window repeat engagement may remain valid if the contract allows gross clicks or repeat clicks.

SECTION 10

GEO, TARGETING, AND CAMPAIGN ELIGIBILITY

Some real clicks are not payable because they fall outside the campaign rules.

10. Geo, targeting, and campaign eligibility

Geography and eligibility issues should be handled carefully. A click outside the target market is not automatically fake. It may come from a real reader traveling, using a VPN, using a corporate network, or being misclassified by IP geolocation. But if the campaign was purchased with specific geography or eligibility terms, the click may still be non-payable.

Eligibility issue	Example	Recommended classification
Outside geography	Campaign is US-only, but click resolves to Germany.	Non-payable if terms require; review if location may be distorted.
Outside campaign date	Click occurs before approved launch or after agreed reporting window.	Non-payable or excluded from final report.
Wrong placement	Clicks came from a link not approved for the campaign.	Non-payable or makegood depending on fault.
Wrong audience	Campaign was contracted for a segment but delivered more broadly.	Review against IO and proof documentation.
Advertiser-specific exclusion	Advertiser excludes data center, incentive, or proxy traffic.	Non-payable if documented in advance.
Advertiser non-payment	Advertiser will not pay for certain traffic or campaign records.	Finance/policy issue; do not call invalid unless evidence supports it.

Why non-payable is not the same as invalid

A real user outside the approved market may be non-payable. A click from an excluded source may be non-payable. A click that violates advertiser-specific terms may be non-payable. None of those automatically prove the publisher generated fraudulent traffic. Clear terminology reduces unnecessary escalation.

> **Practical rule** If the reason for removal comes from campaign terms, call it non-payable. If the reason comes from non-human or duplicate evidence, call it invalid. If the evidence is incomplete, call it unresolved.

Pre-campaign eligibility checklist

- Approved geography and how it will be measured.
- Allowed devices, audience segments, and traffic sources.
- Whether proxy, VPN, data center, or corporate security activity is excluded by policy.
- Campaign dates and time zone for reporting.
- Approved placements, links, creative, and landing pages.
- Final reporting lock date and dispute review window.

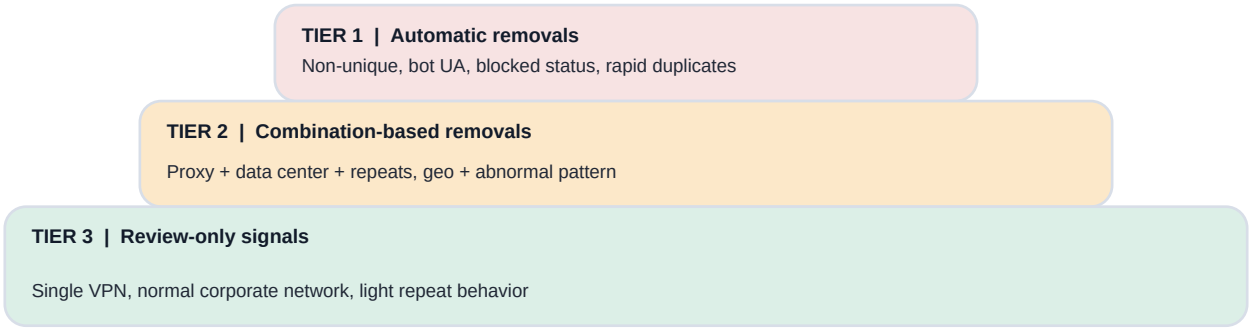
SECTION 11

TIERED REVIEW RULES

A balanced policy removes true invalid clicks without throwing away legitimate readers.

11. How to review click quality without overcorrecting

The goal is not to remove every click that looks unusual. The goal is to remove clicks that are clearly invalid or clearly non-payable under campaign rules. Overcorrecting can be as damaging as under-filtering. If every proxy, VPN, repeat IP, cloud network, or corporate network is removed automatically, valid readers may be lost and publishers may be unfairly penalized.



Use the strongest rule only when evidence is strong. Softer signals need context.

Tier 1: automatic removals

Automatic removals should be reserved for strong invalid evidence: platform non-unique clicks, clear bot or crawler user agents, non-browser automated clients, platform-blocked clicks, rapid duplicate clicks, internal proof clicks, and extreme repeat behavior that is clearly abnormal.

Tier 2: combination-based removals

Combination-based removals apply when softer signals overlap. For example, proxy alone may be kept. Proxy plus data center ASN plus rapid repeat behavior should likely be excluded. Non-US alone may be kept if the campaign has no geo restriction. Non-US plus advertiser US-only terms becomes non-payable. A single corporate network is normal in B2B, but the same network clicking every link at the same timestamp is scanner-like.

Tier 3: review-only signals

Review-only signals should be monitored, segmented, and documented but not automatically removed. These include a single VPN flag, a single cloud/corporate network flag, light repeat IP activity, normal browser behavior on a business network, or non-US geography without a targeting restriction.

Tier	Rule	Examples	Output
Tier 1	Strong evidence	Bot UA, non-unique, blocked status, rapid duplicate, internal proof.	Exclude with code.
Tier 2	Signal overlap	Proxy + data center + repeats; fast click + multi-link sequence.	Exclude or hold after review.
Tier 3	Soft signal only	Single VPN, normal corporate network, light repeats.	Review or keep.

Balanced standard The review policy should be strict where the evidence is strong and conservative where the evidence is weak. That is what makes the process defensible.

SECTION 12

IMPACT ON ADVERTISERS

Invalid traffic can make weak campaigns look strong and strong campaigns look weak.

12. How invalid traffic impacts advertisers

Invalid traffic can distort nearly every metric an advertiser uses to evaluate newsletter advertising. It can inflate clicks, lower the reported cost per click, weaken conversion analysis, create attribution discrepancies, and mislead budget decisions. The surface report can look efficient even when part of the activity did not come from real readers.

Advertiser problem	How invalid traffic distorts it	Better view
Inflated click volume	Gross clicks include bots, duplicates, scanners, or non-human events.	Report gross and validated clicks separately.
Misleading CPC	Invalid clicks make cost per click look lower than it really is.	Calculate CPC on validated or payable clicks.
Weak conversion analysis	Invalid clicks rarely behave like real visitors, so post-click conversion rates can look artificially low.	Analyze conversion rate from valid clicks and sessions.
Platform discrepancies	Newsletter platform, affiliate system, and analytics tools may count different points in the path.	Reconcile adjacent layers.
Bad budget decisions	Advertiser may renew placements with inflated clicks or cut placements that had clean but smaller traffic.	Compare publishers on validated engagement and downstream behavior.

How to report performance honestly

A clean advertiser report does not hide gross activity. It shows the full funnel: gross clicks, removed invalid clicks, validated clicks, sessions, conversions, approved conversions, and final cost metrics. This gives the buyer a better view of what happened and prevents the campaign from being judged on a misleading top-line number.

> **Advertiser-facing language** We separate gross clicks from validated clicks so the final performance view reflects qualified activity, not automated or duplicate interactions. This gives you a clearer basis for CPC, conversion rate, renewal, and budget decisions.

Advertiser questions to answer before launch

- What traffic is eligible for billing and reporting?
- Are clicks validated before final reporting?
- How are security scanners, non-unique clicks, proxies, VPNs, hosting networks, and geo mismatches handled?
- Which platform is the source of truth for clicks, sessions, conversions, and approved outcomes?
- What data will be shared if the advertiser disputes click quality?

SECTION 13

IMPACT ON PUBLISHERS

Traffic-quality review should protect publisher relationships, not just advertiser budgets.

13. How invalid traffic impacts publishers

Invalid traffic does not only hurt advertisers. It also hurts publishers. High-quality publishers rely on trust. If an advertiser questions traffic quality, publishers may face delayed payouts, reduced renewals, lower rates, more aggressive validation requirements, or exclusion from future campaigns.

Publisher impact	What happens	How to reduce risk
Delayed payouts	Payment is held while traffic is reviewed or reconciled.	Monitor quality before statements are finalized.
Reduced payable earnings	Invalid or non-payable clicks are removed from final payout.	Understand validation rules and monitor anomalies.
Loss of advertiser confidence	Advertisers become hesitant to renew or expand budget.	Provide clean send data and cooperate on review.
More operational friction	More questions, proof requests, and manual reconciliation.	Standardize link QA and reporting exports.
Reputation risk	Repeated quality concerns affect future monetization opportunities.	Treat traffic quality as part of revenue operations.

Publisher self-monitoring checklist

- Sudden spikes in clicks or click-through rate that do not match historical behavior.
- Repeated clicks from the same IP, user agent, hashed user, or recipient domain.
- Clicks occurring immediately after send in large clusters.
- High concentration from one geography, ASN, ISP, or device type.
- Traffic from hosting or data center networks.
- Bot, crawler, unknown, or non-browser user agents.
- Low or no post-click engagement for large click clusters.

Publisher-facing tone

When sharing adjustments, avoid broad accusations. State what is supported for payout, what was excluded, and which documented rule was applied. If the issue is scanner activity, describe it as non-human eligibility filtering, not intentional inflation.

Why clean traffic is a monetization asset

Publishers that can show consistent validated click quality, clean audience behavior, and responsive QA will have an advantage as more advertisers treat newsletter advertising as a performance channel. Clean traffic supports stronger renewals, fewer disputes, and better long-term pricing power.

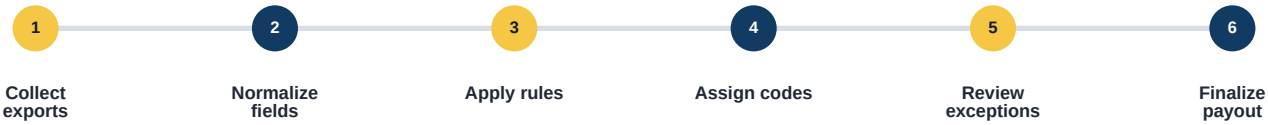
SECTION 14

DEFENSIBLE CLICK REVIEW WORKFLOW

A repeatable review process turns a messy click file into a defensible answer.

14. How to build a defensible click review process

A defensible traffic-quality process is consistent, documented, and easy to explain. It should answer four questions: what signals were reviewed, which signals triggered automatic removal, which signals required overlap, and how final payable clicks were calculated.



A defensible process starts before the send and ends with a locked audit trail.

Step	Action	Output
1	Start with raw click exports from the tracking platform, validation provider, affiliate platform, and analytics tools.	Unmodified raw data saved.
2	Normalize timestamps, publisher names, campaign IDs, countries, user agents, browser fields, ISP/ASN values, and payout rates.	Cleaned review table.
3	Apply automatic removal rules for strong invalid evidence.	Excluded click set with reason codes.
4	Review overlapping risk signals for proxy, VPN, data center, geo, repeat IP, and scanner patterns.	Review bucket and combination removals.
5	Separate invalid removals from non-payable removals.	Clear classification for reporting and payout.
6	Create publisher-level summaries: original clicks, removed clicks, payable clicks, original payout, adjusted payout, and final payable amount.	Publisher statements and finance view.
7	Keep an audit trail of raw file, cleaned file, removed clicks, payable clicks, rules, and final statement.	Defensible package for disputes.

Never overwrite raw tabs. All exclusions should be traceable from raw click to final payable amount.

Required fields for a click-quality review

Field	Why it matters
campaign_id, advertiser, publisher, placement	Connects records across reporting, finance, and partner statements.
send date, send time, click timestamp, timezone	Enables scanner and rapid-repeat detection.
tracking URL and destination URL	Shows approved path and whether redirects changed.
click ID, sub ID, link ID	Supports matching across newsletter, affiliate, and advertiser systems.
IP or hashed IP, ASN, country	Supports traffic source and geo eligibility review.
user agent, browser, device, OS	Supports bot, scanner, and non-browser classification.

Field	Why it matters
validation status and reason code	Documents why clicks were kept or removed.
CPC or payout rate	Translates valid clicks into finance-ready payout totals.

SECTION 15

PLATFORM DISCREPANCY WORKFLOW

Discrepancies are normal. The key is to locate the layer where the gap appears.

15. How to handle discrepancies between platforms

It is common for newsletter reports, advertiser analytics, validation providers, and affiliate platforms to show different numbers. A discrepancy does not automatically mean something is wrong. Different platforms measure different events, use different time zones, apply different filters, and define eligibility differently.

Common platform differences

Comparison	Why it may differ	What to investigate
Gross clicks vs validated clicks	Validation removes bots, scanners, non-unique, duplicate, or ineligible activity.	Reason code breakdown and removed-click sample.
Validated clicks vs affiliate clicks	Affiliate endpoint did not load, parameters were stripped, or network filters applied.	Redirect chain, affiliate ID, click ID, sub ID, network status.
Affiliate clicks vs sessions	Landing page did not load, scripts blocked, consent denied, session definition differs.	GA4/session setup, landing page speed, consent, ad blockers.
Sessions vs conversions	Traffic may be valid but offer, landing page, or audience fit is weak.	Conversion event setup, form errors, message match, CRM records.
Conversions vs approved conversions	Affiliate dedupe, reversals, caps, attribution windows, approval rules, or fraud review.	Network approval status and rejection reasons.

Better wording

Instead of saying 'the numbers do not match,' say: 'The largest gap occurred between gross clicks and validated clicks, driven primarily by scanner-like activity and duplicate clicks. Affiliate capture was stable against the validated click count.'

Discrepancy investigation questions

- Did the click fire in the newsletter platform?
- Did the validation provider keep or remove the click?
- Did the affiliate endpoint load with the required parameters?
- Did the landing page preserve UTMs and click IDs after every redirect?
- Did analytics fire after consent rules and page load?
- Were clicks filtered by affiliate, fraud, geo, device, or advertiser-specific rules?
- Did conversions later become approved, rejected, reversed, or unattributed?

Reporting layer table

Layer	Use this for	Do not use it for
Gross clicks	Top-of-funnel interaction and anomaly detection.	Final CPC or payout if invalid traffic is excluded.
Validated clicks	Quality-adjusted engagement and CPC analysis.	Site session analysis without checking landing behavior.
Affiliate clicks	Network-recognized traffic and attribution setup.	All newsletter engagement if affiliate endpoint failed.
Sessions	Landed traffic and site behavior.	Click counts when scripts, consent, or page load differ.
Approved conversions	Final payable or attributable outcomes.	Diagnosing whether clicks were valid at the top of the funnel.

SECTION 16

INSERTION ORDERS AND PAYOUT RULES

Define what counts before the campaign runs, not after a dispute starts.

16. Best practices for insertion orders, terms, and payout rules

Invalid traffic disputes are much easier to manage when expectations are documented before the campaign begins. The insertion order or terms should define how traffic will be counted, what traffic is not payable, when final reporting is locked, how disputes are handled, and what data may be shared during review.

Term to define	Recommended language direction
Valid click	A unique, human-initiated click that meets campaign requirements and is not filtered by agreed traffic-quality rules.
Gross vs validated clicks	State whether reporting, billing, and publisher payout are based on gross clicks, validated clicks, affiliate clicks, approved conversions, or another metric.
Invalid traffic exclusions	State that automated, non-human, duplicate, scanner, bot, blocked, or invalid activity may be excluded when supported by evidence.
Non-payable traffic	Define traffic outside approved geography, date range, placement, advertiser exclusions, or campaign terms.
Review window	Set a defined period for post-campaign validation and reconciliation before final payout.
Data sharing	Define which records may be shared, such as reason-code counts, publisher summaries, and anonymized examples.
Makegoods	Define eligibility for wrong creative, wrong link, wrong date, wrong audience, or material tracking failure.
Advertiser payment dependency	If publisher payouts depend on advertiser payment, state this clearly and consistently.

Not legal advice This section is operational guidance. Contract language should be reviewed by counsel before being used in live agreements.

Payment model considerations

Model	Risk	Recommended protection
CPC	Gross click inflation can overpay if scanner or invalid traffic is counted.	Base payout on validated clicks or define exclusions clearly.
Flat fee	Advertiser may challenge performance even when delivery obligations were met.	Report validated performance but make payment terms delivery-based unless makegood terms apply.
CPA/affiliate	Publisher may drive traffic but lose attribution to dedupe, cookie windows, or approval rules.	Define attribution window, approval process, reversals, and rejection reasons.
Hybrid	Confusion over base fee, click threshold, and conversion bonus.	Separate guaranteed fee, click target, and bonus logic in writing.

When to credit, hold, or pay

- Credit when a trafficking or link setup issue materially prevented tracking or delivery.
- Do not automatically credit for expected differences between clicks and sessions.
- Do not pay on traffic classified as invalid under the agreed policy.
- Use makegoods when the wrong URL, creative, date, audience, or placement was delivered.
- Hold material unresolved amounts only when data is inconclusive and the financial impact is meaningful.

SECTION 17

DASHBOARDS, TEMPLATES, AND CHECKLISTS

The best review process is repeatable enough to become a dashboard.

17. Dashboards, templates, and operating checklists

A traffic-quality process should not live only in one-off spreadsheets. The same fields, rules, reason codes, and summaries should be repeatable across campaigns. The following modules can be converted into a dashboard, Airtable view, spreadsheet, or platform workflow.

Dashboard view: show gross, valid, invalid, unresolved, and top reason codes before billing or payout decisions.

Dashboard modules

Module	Fields to show	Why it matters
Top-line funnel	Gross clicks, valid clicks, invalid removed, unresolved, payable clicks.	Shows the full review path.
Reason code detail	Counts by NON_UNIQUE, BOT_UA, SCAN_FAST, DC_ASN, PROXY_VPN, GEO_OUT, etc.	Avoids black-box exclusions.
Publisher view	Publisher, placement, send date, original clicks, removed clicks, payable clicks, payout.	Supports partner statements.
Signal concentration	IP/ASN, geo, user agent, timestamp clusters, device, link sequence.	Finds anomalies quickly.
Discrepancy layer	Largest gap layer, gap percent, status, owner, next action.	Directs investigation.
Action log	Issue, owner, fix, deadline, recurrence prevention.	Turns findings into operations.

Pre-send checklist

- Confirm approved advertiser, publisher, placement, run date, and campaign ID.
- Verify final landing URL, tracking URL, affiliate URL, click ID, sub ID, and UTMs.
- Click from an actual proof email on desktop and mobile, not just a copied URL.
- Confirm redirects preserve UTMs and click IDs.
- Confirm analytics, affiliate tracking, and conversion test events fire when permitted.
- Lock links after approval and require change control for updates.
- Document reporting time zone and final reconciliation lock date.

Post-send checklist

- Check first-hour click volume and time-to-click distribution.
- Identify immediate all-link or multi-link scanner patterns.
- Compare gross clicks, validated clicks, affiliate clicks, sessions, and conversions.
- Segment anomalies by publisher, link, device, geography, user agent, ASN, and timestamp.
- Assign reason codes before finance finalizes payout.

Publisher statement template

Line item	What to include
Campaign and run date	Advertiser, publisher, placement, date, rate type.
Original click total	The starting count before validation.
Excluded clicks	Count removed with reason-code category, if sharing is allowed.
Payable clicks	Final clicks eligible for payout.
Rate and final amount	CPC or flat amount and final payable total.
Status	Paid, pending, held for review, or adjusted.

SECTION 18

GLOSSARY AND SOURCE NOTES

Definitions and research references for traffic quality, measurement, and compliance.

18. Glossary

Term	Definition
Bot	An automated system that performs actions online without direct human interaction.
Crawler	A bot that scans or indexes links, pages, or content.
Data center traffic	Traffic that appears to originate from server or cloud infrastructure rather than normal residential, mobile, or business access networks.
Deduplication	The process of counting one event out of multiple similar events according to a defined rule.
Gross click	All recorded click interactions before validation, filtering, or exclusion.
Invalid traffic	Traffic that should not be counted as a legitimate advertising interaction.
Non-payable traffic	Traffic that does not qualify for payment under campaign terms, advertiser rules, or validation policy.
Non-unique click	A click the platform identifies as duplicate or repeat activity rather than a unique interaction.
Proxy	An intermediary server that routes traffic and may obscure the user's original IP or location.
VPN	A virtual private network that routes activity through another server, often for privacy or security.
Rapid repeat click	Repeated click activity from the same source within a short period that may indicate automation or duplication.
Reason code	A standardized label explaining why a click was kept, removed, or placed in review.
Scanner click	A click-like event created by email security or link inspection software rather than a human reader.
Session	An analytics-defined visit or interaction period on a site, not the same thing as a click.
User agent	A string that identifies the browser, device, app, or automated system associated with a click.
Valid click	A unique, human-initiated click that meets campaign requirements and is not filtered by traffic-quality rules.

Source notes

These sources informed the measurement, validation, security, and compliance recommendations in this guide. They are included for research context and should not be treated as legal advice.

Topic	Source
MRC invalid traffic standards	Media Rating Council, Invalid Traffic Detection and Filtration Standards Addendum, June 2020; MRC standards and guidelines page.
MRC 2024 IVT interim update	Media Rating Council, Digital Measurement Vendors Subject to MRC Audit From 2024 IVT Interim Updates, April 2024.
Click measurement	Interactive Advertising Bureau / Media Rating Council, Click Measurement Guidelines, Version 1.0, May 2009.
Clicks vs sessions	Google Ads Help, Clicks and Sessions Discrepancy for Google Ads and Analytics.
Campaign URL parameters	Google Analytics Help, URL builders: Collect campaign data with custom URLs.
Security link rewriting	Microsoft Learn, Safe Links in Microsoft Defender for Office 365.
Unwanted security clicks	Barracuda Networks documentation, Unwanted Link Clicks.
Native advertising disclosure	Federal Trade Commission, Native Advertising: A Guide for Businesses.
Commercial email requirements	Federal Trade Commission, CAN-SPAM Act: A Compliance Guide for Business.

MEDIA INTERCEPT

Make Traffic Quality Part of the Workflow

About Media Intercept

Media Intercept helps brands buy newsletter advertising across premium publishers with better workflow, clearer reporting, and more accountable performance measurement. The platform is built to make newsletter campaigns easier to plan, launch, track, and evaluate while helping publishers monetize their inventory with a more organized and transparent process.

Final takeaway	Remove true invalid clicks. Review suspicious patterns in context. Separate invalid from non-payable traffic. Keep the audit trail. Finalize payouts only after quality review.