ENGLISH · 18 OCTOBER 2026

The Steam Dossier: rules, routes and accountability

Public forensic investigation of Steam OpenID authentication, Valve enforcement, account data access and the market-ceiling economy.

Prepared	18 October 2026
Attribution	PhishDestroy Team
Live article	phishdestroy.io/steam_dossier/
Reading files	PDFs, article JSON and verification

A dated reading edition of the published article. Original evidence, reported claims and editorial interpretation retain the distinctions and limits stated in the text.

READING MAP / 32 SECTIONS

Follow the record.

Article overview 3

Valve's answer to New York: the ownership lie and its framing. 3

The rule. The record. The unanswered questions. 3

The business inside Steam. 5

Open letter to the Washington State Gambling Commission 7

The site is blocked. The login route is not. 8

An endpoint closed. Public tracing lost a key. 25

One session. More access than the user sees. 27

Interactive Exploit & Hijack Simulator 32

The endpoints behind the sequence. 33

A checked box. Whose action? 34

Their rulebook. The recorded platforms. 37

An automation API. A rule against automation. 39

Ten days demanded. Ten years to account for. 40

The hostname is already in the request. 47

The off-Steam price gap 49

Who can reset the safeguards? 52

Follow the money. Separate the transactions. 57

The Digital Services Act: put knowledge on the record 59

Minors: a Steam login is not an age check 61

The request. The reply. The missing comparison. 62

The Subscriber Agreement against the platform's own architecture 66

The findings. The records we ask for. 68

Evidence Memorandum — material provided by Source 1 70

The redaction in the produced PDF is cosmetic: the covered text remains extractable 71

Support and Legal Correspondence Exhibits 73

Selected primary records 73

ArchiSteamFarm and the automation clause 76

Choose a rule. Inspect the matching records. 79

DSAR playbook: request the evidence 79

Support volume. Published response times. 81

Count the records. Check the scope. 85

Valve publishes no enforcement record. We built one. 85

Edition, sources & verification 87

The entries are clickable. The PDF bookmarks provide another route through the document. External source links open the referenced publication or retained file.

AGENT ELISE / VALVE & ENFORCEMENT

Valve's answer to New York: the ownership lie and its framing.

Eight claims beside the documents. Physical collectibles, consumer choice, privacy — and the power Valve retains over accounts and items.

Section 1 — Case briefing

The rule. The record. The unanswered questions.

Context & source limits
Six findings, each tied to a dated public record. The detailed sections follow the same order: technical record (Part A), rules and enforcement record (Part B), legal frameworks (Part C), then the appendices with the primary exhibits.

Six findings. Each connects a written rule to a dated record and a question the evidence can test.

▼ **1. Separate-domain auth hosts — 44 routes · 26 split pairs**
The live register records **44 platforms authenticating through a separate registrable domain**. Six further routes are listed in the saved register's pending-verification group. They remain outside the 44 recorded routes and the registration-age chart until the required RDAP and Link Filter checks are recorded. — **27 with a published per-route evidence file** and 17 added from manual collection, listed apart. In **26 filter-split pairs** the main domain is **BLOCKED** in the Steam Link Filter while the proxy carrying its login is not. These are not burner domains: csgogem.com is blocked while `api.csgem.com`, the host carrying its Steam login, has been registered since March 2014 — **12 years 6 months**. Valve receives that hostname in every OpenID request, and renders it back to the user on its own login page. Full table, per-route ages and sourcing in Section 3.

Follow the route →

▼ **2. 2016: the mechanism was named, the deadline set**
On **13 July 2016** Valve publicly described how gambling sites used Steam OpenID and automated trading accounts, and its counsel's notices of **20 July 2016** set a ten-day deadline. No per-operator enforcement record has been published since. Ten years after that deadline was issued, the same named mechanism is in use on separate-domain auth hosts that returned no Link Filter block on 2026-09-21.

Read the open letter to the WSGC →

▼ 3. Device correlation, on counsel's letterhead

In the correspondence reproduced here, Valve's counsel described device-level correlation linking one device to multiple accounts — a capability Steam Support had previously told users was not technically possible. The open question is which device-level records Valve holds and on what basis account holders are refused access to them.

Read the memorandum →

▼ 4. Two access responses. One withheld the data, one leaked it.

October 2025: Valve's counsel answered an Art. 15 request with an 830-page appendix whose redactions are painted over the text instead of removing it — **902,270 characters** come back out with a standard extraction tool, including the third-party identifiers the bars were there to withhold. Art. 15(4) is the reason those bars exist. **September 2026:** ticket HT-2YBP-F7JP-D4VB was closed after three days with a link to the self-service Account Data page — no data, no stated legal basis. The one-month period under Art. 12(3) had not expired at publication; the objection is to the substance.

Read the redaction check →Read the ticket record →

▼ 5. The market above Steam's ceiling

Steam caps a Market listing at about **$1,800**. Across five marketplaces in a dated snapshot (**23 Sep 2026**), **248 CS2 item categories** are priced above that cap by two or more of them independently, and **all 248 are absent from Steam**; a Factory New Dragon Lore starts at **$10,941** across 389 copies listed on all five (the CSFloat-only figure in Section 13, from the 20 Sep snapshot, is $10,623.95 across 62 offers). Selling at those prices requires an outside venue, while item transfer still runs through Steam.

Follow the price and transfer →

▼ 6. The rule is explicit; the audit trail is not

The Subscriber Agreement reserves Steam for personal, non-commercial use, bars commercial exploitation except as expressly permitted, prohibits scripts and bots, and allows account termination. Valve applied that language to gambling operators in 2016. Separately, according to CSFloat's engineering account, Valve closed `IEconItems_730/GetPlayerItems` in 2017, removing public access to original item IDs (no Valve changelog located).

Put the rule beside the network →

▼ Five claims with direct source links

TL;DR — 5 VERIFIABLE CLAIMS All 5 verifiable against Valve's own servers, documents and published dates

- 44
  platform routes use an authentication host on a different registrable domain from the platform's main address. The unit is a platform route; several platforms share a host.

  Section 3
- 26

filter-split pairs: main domain shows a Steam Link Filter warning; the login host beside it does not.

Section 3.2

- 12y 6m
  is the registration age of `csgem.com` at the September 2026 check. The saved check pairs blocked `csgogem.com` with unblocked `api.csgem.com`.

  View table
- 10 days
  was Valve's own 2016 deadline to gambling operators. No per-operator enforcement record has been published since.

  Section 2
- 830 pp
  Art. 15 GDPR response from Valve's lawyers — 902,270 characters of extractable redactions, redaction bars left as selectable text.

  Section 18

WHAT THIS MEANS — THE STEAM LINK FILTER
Steam's Link Filter returned *"Link Blocked!"* for the main domains in 26 recorded pairs, while the associated authentication hosts returned no block in the saved checks. The Rollbit record separately describes Steam serving its login form for `rbsnin.com`. Valve receives the declared host in the OpenID request: the demand is for its enforcement record against those routes.

11 OCTOBER 2026 / TWELVE NEW CASE FILES

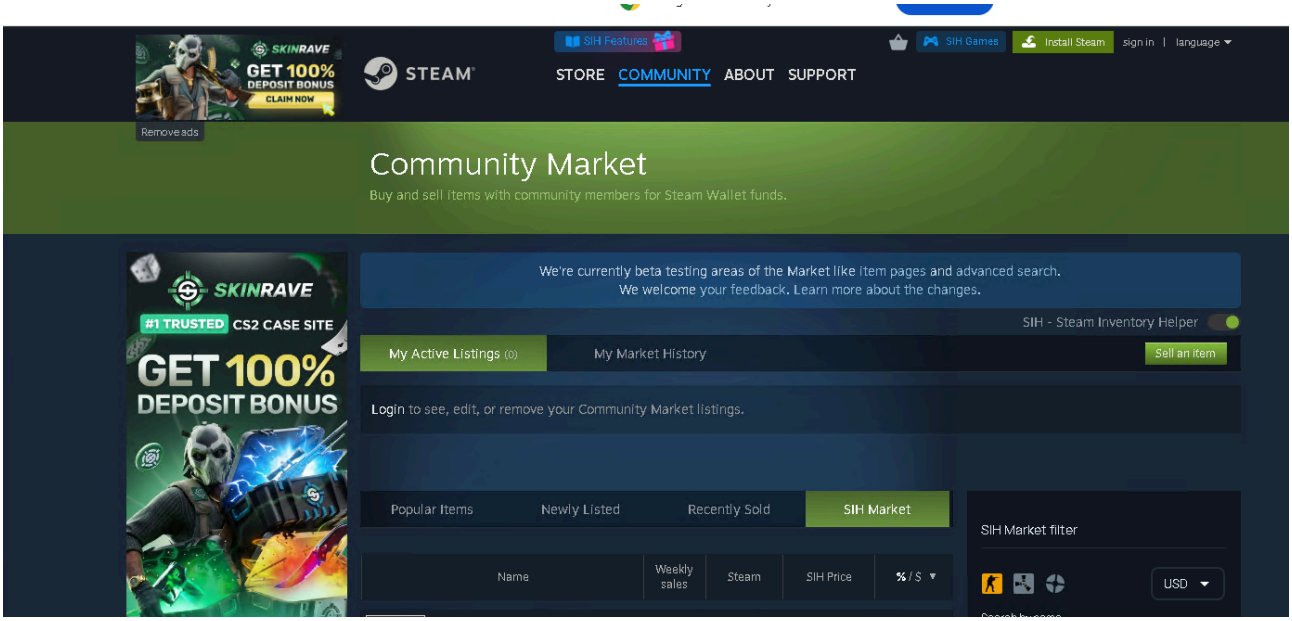
The business inside Steam.

Casino storefronts, account custody, sponsored tournaments and the enforcement record. Follow each part of the investigation.

Commerce & account access

CSGOFast / SIH

Casino commerce, account custody and remote control inside Steam.



AGENT NORA**Read investigation** Reviews & incentives

Reviews & incentives

The contests, ratings and developer replies behind the extension's reputation.

AGENT VERA**Read investigation** Tournament rules

Sponsors & cosmetic control

Tournament restrictions, gambling sponsors and the business of appearance.

AGENT LENA**Read investigation**

▼ **View all 12 investigations**

▼ **Read the original records**



NEW EVIDENCE FILE / SEVEN MAJORS**Their stage. Their skins. Their economy.** *491 maps · 960,770 inspect records · Explore the Major skin dataset*

▼ **Report scope and edition**

2016 / Written demand **10 days**
Deadline in Valve counsel's July 2016 notices to gambling sites. Open letter to the WSGC: Section 2.
2017 / Public audit trail **ID access closed**
CSFloat records the loss of original item IDs.
Counsel correspondence **Device correlation**

One device linked to dozens of stolen accounts.
Route register **Blocked, and still logging in**
The rule: Valve's 2016 statement prohibits running a gambling business on Steam OpenID. **The record:** 26 main domains sit on the Link Filter while the host carrying each one's Steam login runs on — csgogem.com's has run 12 years 6 months.

Section 2 — Open letter

Open letter to the Washington State Gambling Commission

Ten days became ten years. The Commission's 2016 question to Valve has not been answered with an operator-by-operator record; this letter asks it to reopen the file.

PUBLIC ADDRESS · WASHINGTON STATE GAMBLING COMMISSION

Ten days became ten years. *Reopen the record.*

To the Washington State Gambling Commission:

In 2016, Director David Trujillo asked Valve to show what it had done to stop the use of Steam skins for gambling. Then-Chair Chris Stearns and the Commission confronted an industry built on Valve-issued items and Steam transfers. Both men have since left their Commission roles. The question they put to Valve has not expired.

Valve's general counsel, Karl Quackenbush, gave gambling operators ten days to stop commercial use of Steam accounts. In its October response to your Commission, Valve denied facilitating gambling, said it had sent cease-and-desist letters to more than forty sites and said it had disabled associated accounts. It also defended preserving Steam trading and OpenID because those services benefited customers and game developers. **That was an assertion of control. It deserves a test, not deference.**

In our assessment, Valve's answer did not demonstrate that its chosen enforcement matched the scale of the network it described. A threatening letter to an operator is not the same thing as a durable block on the Steam accounts, trading infrastructure and authentication routes that make the business work. Reported estimates put CS:GO Lounge alone above $1 billion in betting handle during 2016; that is an outside estimate of wagers, not Valve revenue, and the site's original skin-betting operation later shut down. The scale made verifiable enforcement essential.

Today, Valve's own Subscriber Agreement archived 2026-09-21 ↗ restricts commercial exploitation except where expressly permitted and separately prohibits specified forms of automation. Our dated route register records declared OpenID return hosts for outside services; `openid.realm` and `openid.return_to` are fields sent to Steam, not secrets hidden from it. Our Link Filter checks show cases where a main address was warned against but an associated login

host was not. A filter result alone cannot prove that Valve allowed a login or that a particular bot evaded an account ban. **It does prove that a homepage warning cannot be offered as a complete answer about access.**

Nor can the existence of useful, lawful Steam trading and OpenID functions answer whether prohibited operators were actually excluded. Valve's own rules allow express exceptions. If Valve relies on that distinction, the Commission should ask it to identify the authorisation, account controls and enforcement criteria applicable to commercial skin businesses, and the specific non-gambling uses it invoked in 2016. The mere possibility of lawful use is no answer to documented prohibited use.

We ask the Commission to revisit its 2016 file and request an operator-by-operator account: which Steam accounts and trading bots were disabled after the ten-day notices; whether related accounts or return hosts were monitored; which operators later regained access; what exemptions were granted; and what records support Valve's statement to the Commission. Publish what law allows the public to inspect. Compare those records with current routes and with Valve's later interventions, including OPSkins in 2018 archived 2026-03-07 ↗.

The notice set a ten-day deadline in July 2016; ten years is long enough to establish whether it was carried out. The Commission should test Valve's 2016 account against the infrastructure that remains observable today.

The Steam Dossier investigation · Public statement, 20 September 2026

2016 Commission notice ↗ archived 2026-05-20 ↗ · Valve's 2016 reply (document copy) ↗ · Valve's 2016 OpenID statement ↗ archived 2026-09-21 ↗ · Current Steam agreement ↗ archived 2026-09-21 ↗ · Timeline of the 2016 exchange: Section 11 →

Part A — Technical record · Section 3

The site is blocked. The login route is not.

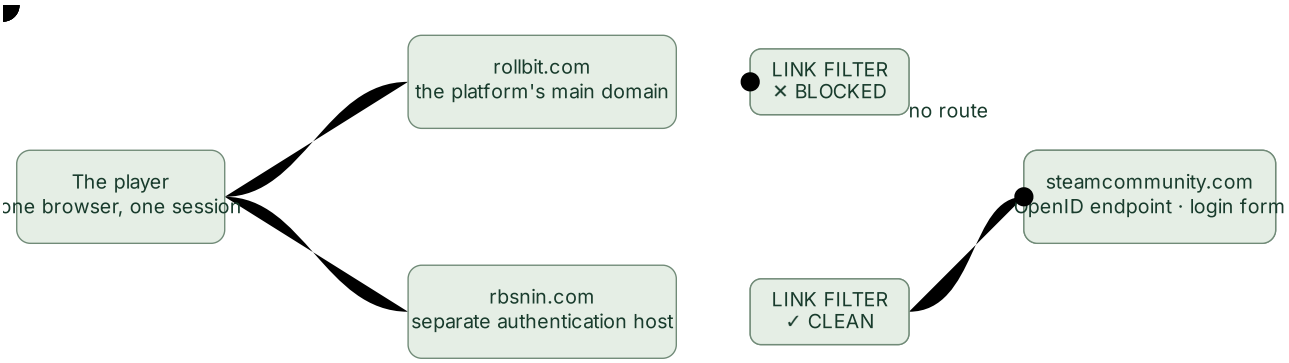
26 blocked main domains, each paired with a separate authentication host that returned no Link Filter block in the saved checks. The register records 44 separate-domain platform routes, with 27 published per-route evidence files and 17 manually collected routes. For CSGOGem, the recorded pairing is blocked `csgogem.com` and unblocked `api.csgem.com`; RDAP dates `csgem.com` to March 2014. Registration age and the date of the observed route are separate measurements. **Valve receives the declared authentication hostname in each OpenID request. It does not have to discover that hostname elsewhere.** Follow the dated checks below, then require Valve to account for the controls it applied to those hosts and operators.

▼ **Inspect the original route illustration**

Figure 3.1 — The two routes, drawn.

Two checks, two results. The saved Link Filter responses compare the platform's main address with its separate authentication host. The login-page observation separately records the route reaching Steam's form.

Swipe the diagram sideways →



Link posted in Steam — stopped Login request — passes Saved checks of 19 and 21 September 2026

The declared host reaches Valve's own endpoint. The saved filter checks show different treatment of the two destinations; the Steam login-page notice records the authentication hostname. These are the records against which Valve's account of enforcement must be tested.

One platform. Two different routes.ROLLBIT / SAVED OBSERVATIONS
01 THE LINK FILTER CHECK
DESTINATION**rollbit.com**The platform's main domain
STEAM LINK FILTER**Checks the link**A separate destination-warning system
SAVED RESULT**Link blocked**19 & 21 September 2026
02 THE OBSERVED SIGN-IN ROUTE
ON THE PLATFORM**Sign in with Steam**The platform starts an OpenID request
SEPARATE AUTH HOST**rbsnin.com**No Link Filter block in the saved check
STEAM**Login form served**The requested host appears in Steam's notice
The request reaches Steam. The observed route reached Steam's login form. The authors did not complete the login. Blocking the main-domain link did not block this observed route to the form.

Inspect the original capture notes, registration date and protocol details
What Valve's enforcement looks like
Main domain: blocked
User
→
rollbit.com
(main domain)
↓

STEAM LINK FILTER — BLOCKED
"Link Blocked!" — flagged as potentially malicious
rollbit.com returned a Link Filter block on 2026-09-19 and 2026-09-21 (unauthenticated check; raw HTML and SHA-256 saved). A visible, auditable record.
What actually happens — authentication
Auth host: not blocked
User
→
rollbit.com
"Sign in with Steam"
↓
Redirect via separate auth host:
`rbsnin.com`Link Filter: CLEAN
registered 2026-09-18T09:34:52Z (Verisign RDAP)
↓
Steam login page notice (2026-09-20):
`"Note that rbsnin.com is not affiliated with Steam or Valve"`
Steam renders this notice from the openid.realm of the request it received.
↓
Steam login form served for the separate host
The login was not completed by the authors; the flow was observed up to the Steam form. Valve receives the return_to / realm hostname on every such request. rbsnin.com returned no Link Filter block on 2026-09-21.
Per request
As the OpenID provider, Steam receives the auth hostname with every authentication request: it arrives at Valve's own servers in the `openid.return_to` and `openid.realm` parameters.
Sent by the site
The auth host is not discovered by scanning — the platform sends it to Steam in each request. Under OpenID 2.0 §9.1 `return_to` is formally optional, but without it Steam cannot deliver the login result, so for a working Steam login it is effectively required. Steam even renders the hostname to the user ("*<host> is not affiliated with Steam or Valve*").
14 yr
is the registration age of `dota2.net`, registered 29 October 2011 and listed as an authentication host in the September 2026 register. `rbsnin.com` was three days old at the 21 September check. These dates describe the domains' registrations. The paired filter checks and login observations are dated separately below.

Separate-domain auth hosts: registration date vs. main domain (30 routes: the 25 resolved in the 2026-09-21 browser audit, plus 5 added on 2026-09-22)

Read the counts against the same register.

44
Separate-domain platform routes in the saved register.

26
Main-blocked / auth-unblocked pairs within those 44 routes.

30
Rows displayed in the comparison table below.

6
Additional pending routes, excluded from the 44.

22 September register ↗ · Route observation records ↗
The 30 displayed rows are a documented subset. Their counts and coverage must be read separately from the full register.

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Evidence file
Rollbit rollbit.com · reg. 2014-11-08	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	`rbsnin.com`	CLEAN 2026-09-21 · raw HTML (no Wayback snapshot)	2026-09-18 09:34:52Z, Verisign RDAP	Steam login-page notice, 2026-09-20	rollbit.com.json
Skin.Club skin.club · reg. 2017-09-04	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	`sc-auth.net`	CLEAN 2026-09-21 · Wayback 2026-09-21	2019-04-02 RDAP	Steam login-page notice	skin.club.json
Howl.GG howl.gg · reg. 2017-03-16	BLOCKED 2026-09-18, 09-19, 09-21 · Wayback 2026-09-21	`howl.uno`	CLEAN 2026-09-21 · Wayback 2026-09-21	2026-08-11 RDAP	Live browser capture + supplied OpenID URL	howl.gg.json
Duelbits duelbits.com · reg. 2020-02-03	BLOCKED 2026-09-21 · Wayback 2026-09-21	`switchflips.com`	CLEAN 2026-09-21 · Wayback 2026-09-21	2020-04-21 RDAP	Supplied OpenID URL	duelbits.com.json
CSGOFast csgofast.com · reg. 2015-03-27	BLOCKED 2026-09-19, 2026-09-21 · Wayback 2026-09-21	`steam-login.authtofast.com`	CLEAN authtofast.com, 2026-09-21 · Wayback 2026-09-21	2026-06-30 authtofast.com, RDAP	Live browser capture + supplied OpenID URL	csgofast.com.json
Farmskins farmskins.com · reg. 2016-03-23	BLOCKED 2026-09-19, 2026-09-21 · raw HTML	`steam.kobal.cc`	CLEAN 2026-09-19, 2026-09-21 · raw HTML	2017-01-07 kobal.cc, RDAP	Live browser capture + supplied OpenID URL	farmskins.com.json

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Evidence file
CobaltLab cobaltlab.tech	BLOCKED 2026-09-21 · raw HTML	`cobaltauth.com`	CLEAN 2026-09-21 · raw HTML	2025-01-07 RDAP	Supplied OpenID URL	cobaltlab.tech.json
CSGO.NET csgo.net · reg. 2012-07-22	BLOCKED 2026-09-21 · raw HTML	`cn2.easylot.net`	CLEAN 2026-09-21 · raw HTML	2016-09-03 easylot.net, RDAP	Live browser capture	csgo.net.json
GGDrop ggdrop.com	BLOCKED 2026-09-21 · raw HTML	`ggauth.com`	CLEAN 2026-09-21 · raw HTML	2023-05-03 RDAP	Supplied OpenID URL	ggdrop.com.json
RustChance rustchance.com	BLOCKED 2026-09-21 · raw HTML	`hgfuihd.com`	CLEAN 2026-09-21 · raw HTML	2019-01-27 RDAP	Supplied OpenID URL	rustchance.com.json
Skin.Fans skin.fans	BLOCKED 2026-09-21 · raw HTML	`auth.skinfans.com`	CLEAN 2026-09-21 · raw HTML	2018-07-16 skinfans.com, RDAP	Supplied OpenID URL	skin.fans.json
Skinport skinport.com · reg. 2018-09-05	BLOCKED 2026-09-21 · raw HTML	`skinport.app`	CLEAN 2026-09-21 · raw HTML	2020-06-20 RDAP	Live browser capture + supplied OpenID URL	skinport.com.json
Skins.Cash skins.cash	BLOCKED 2026-09-21 · raw HTML	`skinscash.live`	CLEAN 2026-09-21 · raw HTML	2019-12-05 RDAP	Supplied OpenID URL	skins.cash.json
TF2Hunt tf2hunt.com · reg. 2018-01-13	BLOCKED 2026-09-21 · raw HTML	`rstspcl.com`	CLEAN 2026-09-21 · raw HTML	2020-08-08 RDAP	Live browser capture + supplied OpenID URL	tf2hunt.com.json
CSGOGem csgogem.com · reg. 2016-10-16	BLOCKED 2026-09-22 · raw HTML	`api.csgem.com` csgem.com — separate registrable domain	CLEAN 2026-09-22 · raw HTML	2014-03-08 csgem.com, RDAP — oldest in register	Manual collection + Link Filter capture	linkfilter-2026-09-22.json
Gamdom gamdom.com · reg. 2016-07-29	BLOCKED 2026-09-22 · raw HTML	`login.gambldom.com` gambldom.com — one letter off the brand	CLEAN 2026-09-22 · raw HTML	2017-09-24 gambldom.com, RDAP	Manual collection + Link Filter capture	linkfilter-2026-09-22.json
12CS 12cs.fail · reg. 2026-03-24	BLOCKED 2026-09-22 · raw HTML	`fail.games`	CLEAN 2026-09-22 · raw HTML	2021-08-24 fail.games, RDAP	Manual collection + Link Filter capture	linkfilter-2026-09-22.json

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Evidence file
CSGOEmpire csgoempire.com · reg. 2015-06-10	CLEAN 2026-09-19, 2026-09-21 · Wayback 2026-09-21	`csgoempirelogin4.com` one of ten numbered domains login1–10	CLEAN 2026-09-21 · Wayback 2026-09-21	2020-07-20 05:49:17Z, Verisign RDAP	Live browser capture	csgoempire.com.json
CS.MONEY cs.money	CLEAN 2026-09-21 · raw HTML	`auth.dota.trade`	CLEAN 2026-09-21 · raw HTML	2016-07-15 dota.trade, RDAP	Steam login-page notice	cs.money.json
CSFloat csfloat.com · reg. 2021-07-11	CLEAN 2026-09-21 · raw HTML	`csgofloat.com` operator's former brand domain; separate registrable domain, not an evasion indicator	CLEAN 2026-09-21 · raw HTML	2015-09-29 RDAP	Live browser capture	csfloat.com.json
G4Skins g4skins.com	CLEAN 2026-09-21 · raw HTML	`auth.g4s.to`	CLEAN 2026-09-21 · raw HTML	2021-05-30 g4s.to, RDAP	Supplied OpenID URL	g4skins.com.json
Juice.GG juice.gg	CLEAN 2026-09-21 · raw HTML	`letmeinjuice.com`	CLEAN 2026-09-21 · raw HTML	2024-04-15 RDAP	Supplied OpenID URL	juice.gg.json
Market.CSGO market.csgo.com	CLEAN 2026-09-21 · raw HTML	`dota2.net`	CLEAN 2026-09-21 · raw HTML	2011-10-29 RDAP	Live browser capture + supplied OpenID URL	market.csgo.com.json
Rust.TM rust.tm	CLEAN 2026-09-21 · raw HTML	`dota2.net`	CLEAN 2026-09-21 · raw HTML	2011-10-29 RDAP	Supplied OpenID URL	rust.tm.json
CSGOLounge csgolounge.com · reg. 2013-08-14	CLEAN 2026-09-22 · raw HTML	`dota2.net` third front-end on this auth host	CLEAN 2026-09-22 · raw HTML	2011-10-29 dota2.net, RDAP	Manual collection + Link Filter capture	linkfilter-2026-09-22.json
Dota2Lounge dota2lounge.com · reg. 2012-08-10	CLEAN 2026-09-22 · raw HTML	`dota2.net` fourth front-end on this auth host	CLEAN 2026-09-22 · raw HTML	2011-10-29 dota2.net, RDAP	Manual collection + Link Filter capture	linkfilter-2026-09-22.json
SkinBaron skinbaron.de	CLEAN 2026-09-21 · raw HTML	`skinbaron.com` same brand, different TLD	CLEAN 2026-09-21 · raw HTML	2015-12-22 RDAP	Supplied OpenID URL	skinbaron.de.json

Platform	Link Filter: main	Auth host	Link Filter: auth host	Auth host registered	Source of observation	Evidence file
TF2Royal tf2royal.com · reg. 2022-08-17	CLEAN 2026-09-21 · raw HTML	`tf2auth.com`	CLEAN 2026-09-21 · raw HTML	2021-07-27 RDAP	Live browser capture + supplied OpenID URL	tf2royal.com.json
Tradeit tradeit.gg	CLEAN 2026-09-21 · raw HTML	`connect-tradeit.com`	CLEAN 2026-09-21 · raw HTML	2022-02-23 RDAP	Supplied OpenID URL	tradeit.gg.json
Upgrader upgrader.pro	CLEAN 2026-09-21 · raw HTML	`upgauth.space`	CLEAN 2026-09-21 · raw HTML	2026-08-14 RDAP	Supplied OpenID URL	upgrader.pro.json

Source: steamcommunity.com/linkfilter, unauthenticated GET, 2026-09-21, 53 hosts, 3 s spacing; steam_tos_assets/linkfilter-recheck-2026-09-21.json; raw HTML in `steam_tos_assets/linkfilter-raw/`. Registration dates: RDAP, steam_tos_assets/domain-registration.json. · Earlier check of 2026-09-19 in linkfilter-all-results.json · route records in auth-route-audit.json · Wayback Machine snapshots of the Link Filter pages, 2026-09-21, listed in wayback-snapshots.json (no snapshot exists for rbsnin.com; the local raw file is the only record).

Registration dates: RDAP (`steam_tos_assets/domain-registry/`). "Supplied OpenID URL" establishes the request parameters, not a completed login. No login was completed by the authors on any platform. A separate domain is not by itself proof of evasion. Nor is "0 auth hosts blocked" an independent finding: blocking one would break that platform's Steam login, so a register assembled from working logins cannot contain a blocked auth host. The observation that carries weight is the dated pairing: a main domain on the Link Filter beside an authentication host that returned no block. RDAP supplies the separate registration date. This table carries 30 rows: 25 of the 27 routes with a per-route evidence file, plus five added on 2026-09-22 whose Link Filter split is captured in linkfilter-2026-09-22.json even though the realm itself was hand-collected — their rows say so in the source column. The two evidence-file routes not shown are skinsnipe.com (auth host `pricing.tradeupspy.com`, registered 2020-03-11) and csgobig.com (auth host `letmeinbig.com`, registered 2023-01-20); both returned BLOCKED main / CLEAN auth host in the check of 2026-09-22, recorded with SHA-256 in linkfilter-2026-09-22c.json, but the raw HTML for that batch is not in the published set, so they are named here rather than given a row that every other line in this table can evidence. The remaining 12 hand-collected routes in the register are identified as such in master_registry.json under `realm_src: user`.

`Part A — Technical record · Section 3.1`

Inside Steam, Valve’s list is the only list.

A link clicked in the Steam client, the in-game overlay or Big Picture mode does not open in the user's browser. It renders inside Steam's own embedded browser — where the warning layers a browser would apply are not present. **The Link Filter is not one safeguard among several. It is the whole of it.**

In a normal browser Three independent layers

1. **Google Safe Browsing**A full-page interstitial for hosts on Google's phishing and malware lists, updated continuously and independent of the site being visited.
2. **The antivirus browser extension**Most consumer endpoint products ship a browser add-on that checks the destination against the vendor's own reputation list.
3. **Endpoint HTTPS inspection**Where the product performs TLS inspection, page content is scanned before it reaches the user.

In the Steam client, overlay and Big Picture One layer

1. **Google Safe Browsing**Not present. The check requires Google API keys that are not provisioned in embedded Chromium builds; where they are absent, Chromium's own design documentation records that the Safe Browsing handler is simply never added to the request chain.
2. **The antivirus browser extension**Not present. Steam's renderer is not the user's browser and loads no extension from the user's browser profile, so no add-on runs against the page.
3. **Endpoint HTTPS inspection**Product-dependent. The traffic terminates inside a code-signed Valve process rather than a recognised browser, and a number of endpoint products exempt signed applications from TLS inspection.
4. **The Steam Link Filter**Valve's own blocklist, consulted when a link leaves the Steam ecosystem. This is the sole check that runs — and the table above records what it returns for the auth hosts documented in this section.

A test any reader can run, and the finding falls if it fails
Open one of Google's published Safe Browsing test URLs (`testsafebrowsing.appspot.com`) in Chrome: a full-page red interstitial appears. Open the same URL from a Steam chat message, so that it renders in the Steam client or the overlay: no interstitial appears. The only warning Steam can produce is its own Link Filter page, and only for hosts on Valve's list.

Valve's own bug-bounty record**The one layer has been got around before — on Valve's own record**
If the Link Filter is the only check that runs inside the client, its own failure modes are not a side issue. Two reports on Valve's HackerOne programme, both accepted, both resolved, both since disclosed in full:

1. #291750 archived 2025-11-16 ↗Open Redirect · medium

   ### Link filter protection bypass

   Reported 19 November 2017, resolved, disclosed 9 May 2018. The report's own proof of concept: substituting the ideographic full stop 。 (`%E3%80%82`) for the dot in a hostname — “it is possible to bypass the blocking.” The interstitial this section is about did not appear.

2. #1079561 archived 2026-09-24 ↗Information Disclosure · high

   ### Big Picture web browser leaks login cookies and discloses sensitive

information (may lead to account takeover)

Reported 15 January 2021, resolved, disclosed 21 September 2021. Valve's own severity rating is high, and the title states the consequence. The disclosed record carries the title, rating and dates; the technical write-up is not in the published payload, so nothing further is quoted from it here.

The authors' reading, not a finding of either report: the two sit on either side of the same gate. One is the warning failing to appear before the destination opens; the other is the session leaving the client once a page is open inside it. The sequence that follows a stolen session — key registered without a prompt, the real trade cancelled, a duplicate sent to a clone — is the pattern set out in Section 5 to Section 8. Both reports are closed; neither is offered as a live vulnerability. What they establish is narrower and enough: the single remaining layer has a documented history of being got around, on Valve's own record.

Source: the HackerOne disclosure record for each report, retrieved 2026-09-22 — number, title, team, weakness, severity, report and disclosure dates and state as published by HackerOne. Retrieval record: hackerone-reports.json. No bounty figure is stated here; none appears in the disclosed record retrieved.

Field observation · PhishDestroy**Detections that normally end a campaign did not end these** We watched phishing hosts keep pulling traffic while carrying **20 or more vendor detections**. Delivered by web or email, a campaign in that state dies in days — the browser and the antivirus both act on those verdicts. Inside Steam neither does. The verdicts existed the whole time. Nothing in the client ever asked.

What this means for a minor with an antivirus installed

He ignores no warning and disables nothing. A message arrives inside Steam — a free knife, a vote for a friend's team — and the page opens inside Steam. He never opens a browser, so the browser never protects him. His antivirus is running and may already rate that domain malicious; it is never asked. **Every warning that could have stopped him already exists. None of it reaches him.** He believes he never left Steam, and he did not.

The giveaway is not the phisher's invention — free Valve items are how the skin and gambling sites advertise, which is exactly why the message reads as ordinary. Complaints: the enforcement archive. Age and children's data: Section 17.

Sources: Steam renders web content through the Chromium Embedded Framework in the `steamwebhelper` process — see DARKNAVY's technical analysis of 27 June 2024 ↗ and Valve's own Steam Client Beta forum ↗ archived 2025-08-04 ↗. No CEF version is relied on: embedded Chromium is not Chrome and ships none of Chrome's Google services. Safe Browsing without API keys: Chromium design document ↗ archived 2026-08-21 ↗, Chromium API keys ↗ archived 2026-08-30 ↗ (“Many of the Google APIs used by Chrome are specific to Google and not intended for use in derived products”), and the same effect in other unkeyed builds — Homebrew cask #193814 ↗. Test URLs: testsafebrowsing.appspot.com ↗.

`Primary Empirical Audit · Multi-Year Date Range`

The Big Picture Trap: Link Filter is Compliance Theater, Not a Shield

On desktop browsers, users are shielded by external defenses: Google Safe Browsing and Microsoft SmartScreen intercept known phishing with full-screen red warnings. **Inside Steam's Big Picture mode, the in-game overlay (Shift+Tab), and the Steam Deck (SteamOS), those defenses do not exist.** The embedded browser supports zero extensions, disables external Safe Browsing engines, and leaves the user with exactly one defensive barrier: Valve's `linkfilter` interstitial.

Targeted Steam sample: the 120 hosts in these three cohorts were selected for Steam phishing through favicon searches and checks for copied Steam sign-in or home-page interfaces. This deliberate selection is separate from the mixed public-list checks below.

Swipe to compare all four results →

92.5%
2025–2026 modern edge phishing **passed clean** (37/40)
77.5%
2023–2024 CS2 era phishing **passed clean** (31/40)
70.0%
2021–2022 legacy phishing **passed clean** (28/40)
7 / 7
gambling mains blocked (positive control)
Multi-Year Longitudinal Audit: 120 Pure Steam Phishing Domains Tested Live (24 Sep 2026)
To test whether Valve's filter is simply slow to ingest new threats or fundamentally blind to them, we audited **120 confirmed Steam-specific phishing domains** across three historical cohorts against `steamcommunity.com/linkfilter`:

- **Cohort 1: 2021–2022 (Classic Trade-Offer & Item Drops) — 70.0% Clean Pass (28/40).** Even 4 to 5 years after being cataloged by community watchdogs, 7 out of 10 legacy phishing hosts still open without any block.
- **Cohort 2: 2023–2024 (CS2 Beta Hype & Fake Support Appeals) — 77.5% Clean Pass (31/40).** Campaigns impersonating Counter-Strike 2 releases and fake community appeals (e.g. `cs2-steam.com`, `appealsteamcommunity.help`) pass straight through.
- **Cohort 3: 2025–2026 (Serverless Edge Deploys & Favicon Clones) — 92.5% Clean Pass (37/40).** Modern phishing kits deploying on EdgeOne, Vercel, and Cloudflare Pages (e.g. `steamgifter.online`, `steam-dp4lt5b8fnez.edgeone.dev`) pass virtually unobstructed.

Additional public-list checks · 6 October 2026

1,088,753 distinct hosts

Additional analysis of public lists: we did not find a suitable Steam-only public list for a larger census, so we checked lists we considered relevant. None is exclusively Steam scams or phishing; their results are reported separately.

Steam Link Filter responses · percentage of all hosts in each list

List	Tested hosts	Blocked	Blocked %	Ordinary notice
Steam / Discord feeds	36,724	1,759	4.79%	34,965
PhishDestroy · community + main list	1,086,734	4,010	0.37%	1,082,629

Scroll horizontally to compare the results.

Why these lists?

- **Steam / Discord feeds.** DevSpen and Discord-AntiScam cover gaming-account phishing and related scams. They are close to the Steam ecosystem, but the combined list is not exclusively Steam phishing. DevSpen · Discord-AntiScam.
- **PhishDestroy · community + main list.** Our PhishDestroy community and main lists test broader phishing and scam coverage, including crypto. The supplied results also contain blocked crypto-themed hosts, such as `app-metamask-kyc-auth.com`, `app-trezor-auth.com`, so this is a relevant additional check, not a Steam-only sample. PhishDestroy destroylist.

The two runs contain 1,123,458 host records, with 34,705 hosts in both lists: 1,088,753 distinct hosts after deduplication. We do not pool their block rates.

▼ **Method & verification**

Blocked % = BLOCKED ÷ all tested hosts in that row. The PhishDestroy run also has 78 ERROR, 15 UNKNOWN and 2 INTERNAL results; these 95 are included in the denominator, not counted as ordinary notices. The Steam / Discord run has no residual statuses.

ALLOWED means the ordinary “You are leaving Steam” notice was recorded, not that the destination is safe. These dated results measure the supplied lists; they do not establish that every site was still active or how Valve maintains its filter.

Methodology · English · TXT

Recounted results · JSONIndividual files & signatures · English

Telemetry & Liability Shield, Not Protection. Why does the Link Filter exist if it passes 70% to 92.5% of pure Steam phishing? It functions as a corporate liability disclaimer and an outbound click telemetry sensor. By presenting a polite *"You are leaving Steam"* notice with a clickable green proceed button, Valve shifts legal blame onto the victim under the Steam Subscriber Agreement (*"the user voluntarily navigated outside Steam"*). Valve collects the telemetry of the click, but does not block the theft.

The Favicon Hash Proof: Zero Ingestion of Threat Feeds. Independent threat intelligence platforms (urlscan.io, Shodan, Censys) identify live Steam phishing kits using a simple search for Steam's official favicon hash (`page.favicon.hash:9f890a9debcdfccc339149a7943be9aff9e4c9203c2fa37d5671a5b2c88503ad NOT domain:*.steampowered.com`). This basic automated check surfaces active phishing clusters in

seconds. Valve does not sync with external feeds, does not run hash-based threat hunting, and only manually intervenes when compelled by regulators (the 2016 WSGC gambling order) or to protect its trademarked domain strings.

Primary audit evidence artifacts: Longitudinal 120-domain multi-year audit: longitudinal-steam-phishing-audit.json · 100 dedicated Steam phishing sample: linkfilter-steam-phishing-100.json · Broad feed audit (n=250): linkfilter-coverage-2026-09-22.json.

CSGOEmpire — batch registration of ten numbered auth domains

On **2020-07-20** ten numbered domains, `csgoempirelogin1.com` through `csgoempirelogin10.com`, were registered. Verisign RDAP timestamps are on file for all ten: login1 05:49:06Z, login5 05:49:08Z, login2 05:49:11Z, login3 05:49:14Z, login4 05:49:17Z, login6 05:49:20Z, login7 05:49:23Z, login8 05:49:26Z, login9 05:49:28Z — **nine domains in 22 seconds** — and login10 at 05:56:03Z, seven minutes later. The spacing is consistent with a single registrar bulk operation.

The pattern is consistent with pre-provisioned fallback hosts; only `login4` has been observed in a live OpenID request. csgoempire.com and csgoempirelogin4.com both returned CLEAN in the Link Filter on 2026-09-21; CSGOEmpire was not among the sites named in press reports of the July 2016 notices.

DNS — all 10 active (September 2026)
OK csgoempirelogin1.com 172.67.129.43
OK csgoempirelogin2.com 172.67.175.168
OK csgoempirelogin3.com 188.114.96.3
OK csgoempirelogin4.com 188.114.96.11 ← in OpenID traffic
OK csgoempirelogin5.com 172.67.160.194
OK csgoempirelogin6–10.com Cloudflare IPs
NXDOMAIN: csgoempirelogin11.com
All 10 registered 2020-07-20; all 10 RDAP-timestamped (steam_tos_assets/domain-registry/csgoempireloginN.com.rdap.json)

Conclusion for regulators

A blocked main domain paired with an unblocked auth host leaves the login route open — and it stays open for years.

The Link Filter block on the main domain is a verifiable, public record. The auth host carries the "Sign in with Steam" traffic and appears in Valve's own OpenID request parameters. Across checks on 2026-09-21 and 2026-09-22, in 26 filter-split pairs the main domain returned a Link Filter block while the proxy carrying its login returned none. The register above measures the other half of that: these hosts are not short-lived burner domains. Several had been registered for more than a decade at the date of the check, and every one of those days is a day on which Valve received the hostname in its own request parameters. Valve has published no per-operator enforcement record, so whether any other measure was applied to these hosts cannot be established from public data.

12 yr 6 mo

csgogem.com is blocked in the Link Filter.
Its login host `api.csgem.com` has been
registered since 2014-03-08 and is not.

Plain Language Summary — For Regulators & Courts (expand)

`Plain language summary — for regulators`

Background: What Steam Is and Why It Matters Here

Steam is a software platform operated by Valve Corporation (Bellevue, Washington, USA). Steam functions as a digital identity provider: gambling and gaming websites across the internet use a system called "Sign in with Steam" — a button that allows a website to verify that a visitor has a real Steam account. This is similar to "Sign in with Google" or a government-issued identity card check: the website sends the user to Steam's servers, Steam confirms who they are, and Steam sends them back to the website. **Valve operates the authentication system. Every single login through "Sign in with Steam" passes through Valve's own servers.**

What Valve Did: The Domain Block

In July 2016, following media and legal pressure over skin gambling, Valve's counsel sent notices to approximately 23 named gambling sites (per press reports of 21 July 2016); in October 2016 Valve told the Washington State Gambling Commission it had contacted more than forty sites. Some gambling domains appear in the **Steam Link Filter** — a list that makes any link to them posted inside Steam (in chat, on a profile page, in the store) show a warning page: *"Link Blocked!"* The Link Filter is the only enforcement measure whose effect can be observed from outside Valve.

Example: A link to `rollbit.com` inside Steam produces the Link Filter warning page (checked 2026-09-19 and 2026-09-21). On paper, the gambling site is blocked.

What a Proxy Domain Is

A **separate-domain auth host is an authentication proxy**: a second website address, on a different registrable domain, that the same operator puts between its users and Steam for the sole purpose of carrying the "Sign in with Steam" step. It proxies the login. The user believes they are signing in to the platform; the request that reaches Valve carries the proxy's hostname, not the platform's. It usually has no publicly visible connection to the gambling site, and it is the address that receives users back after Steam confirms their identity.

Example: Rollbit operates under `rollbit.com`, which the Link Filter blocks. For Steam authentication, the flow observed on 2026-09-20 used a separate address: `rbsnin.com`, registered 2026-09-18. This address returned **no Link Filter block** on 2026-09-21. The gambling site continued to operate, and its Steam login flow ran through the unblocked host.

The Critical Point: The Auth Host Is Sent to Steam in Every Request

Valve does not need to scan or crawl to learn which auth hosts are in use. Steam is the **OpenID identity provider** for these sites, and every "Sign in with Steam" click sends a GET request to Valve's own servers containing the auth hostname in plaintext. Under OpenID 2.0 §9.1 the `return_to` field is formally optional, but without it Steam cannot deliver the login result, so for a working Steam login it is effectively required. Steam itself renders the hostname on the login page ("*<host> is not affiliated with Steam or Valve*").

— Shape of the request Steam receives (host as observed for Rollbit on 2026-09-20): —
GET steamcommunity.com/openid/login
&openid.mode=checkid_setup
&openid.return_to=https://rbsnin.com/... ← effectively required; arrives in Valve's log
&openid.realm=https://rbsnin.com ← self-declared by the site; rendered on Steam's login page
If the site uses server-to-server verification (check_authentication), Valve's log also records the platform's server IP and hosting network.
Extracting the hostname from this request is a standard operation. The enforcement record — which hosts were acted on, which were not, and under what criteria — exists only in Valve's infrastructure and has not been published.

What This Proves

1. The Link Filter block acts on links, not on logins. Blocking the main domain (for example `rollbit.com`) shows a warning to users who click links to it inside Steam. It does not stop the site from operating, or from using Valve's own OpenID service through a different address.

2. The auth hosts tested were not blocked. The table above shows separate-domain auth hosts registered between 2011 and September 2026, several of them years after the July 2016 notices. In 26 pairs the main domain returned a Link Filter block and the proxy carrying its login did not (unauthenticated checks, 2026-09-21 and 2026-09-22; raw responses and SHA-256 saved). That proxy would stop working the day Valve refused it, which is why the measure here is how long it has run, not whether it is listed. Valve receives these hostnames in its own OpenID requests. Whether any measure other than the Link Filter was applied cannot be determined from public data, because Valve has published no per-operator enforcement record.

3. The sites continued to authenticate through Valve's infrastructure. "Sign in with Steam" is Valve's service; every authentication through it is a request Valve receives and processes. Valve also earns revenue from case keys, and the Steam Community Market charges a combined fee of about 15% on transactions completed inside the Market (not on external trades). The Link Filter action created a public record; it did not interrupt the authentication relationship.

Would Blocking Have Worked?
By analogy: when the free domain registrar Freenom wound down in 2023, phishing campaigns that depended on its domains were disrupted. Operational continuity depends on infrastructure stability.

The same logic applies here. If an auth host were refused in Steam's OpenID processing, the platform's "Sign in with Steam" function would break until a new host is registered, certificates issued and DNS propagated. During that window: downtime.

Rotation does not make blocking futile. It makes blocking an operational cost. Since new hosts appear in Valve's own request logs on first use, a response could run at the speed of that first use.

Batch registration is itself a signal: CSGOEmpire's login1–login10 were registered on 2020-07-20, nine of them within 22 seconds (Verisign RDAP). A response does not need to be domain-by-domain; a sequential series from one registrar session can be identified as a series.

The public record does not show an attempt to block auth hosts that was defeated by rotation. It shows main domains blocked while the proxy carrying each login kept running — 26 pairs as of 2026-09-22, the oldest auth host registered 12 years 6 months — and no published enforcement record for any operator.
The question for the regulator is therefore: what enforcement, if any, has Valve applied to the auth hosts it receives in its own OpenID requests?
What Valve Did — and Why It Did Not Interrupt the Auth Path
The table below maps each publicly documented Valve action against whether it affected the OpenID authentication entry point. The finding is not "Valve did nothing" — it is that none of the publicly documented actions touched the point where gambling-platform logins pass through Valve's servers.

Date	Valve Action	Affected `openid.return_to` path?
July 2016	Public statement of 13 July 2016; counsel's notices to ~23 named sites (press, 21 July 2016); >40 sites contacted per Valve's October 2016 letter to WSGC	No. Notices and the Link Filter act on operators and links; the OpenID request path was not changed.
2017	Closure of `IEconItems_730/GetPlayerItems` (according to CSFloat's engineering account; no Valve changelog located)	No. Affected public item-history visibility. OpenID authentication was not modified.
2018-03-29	CS:GO 7-day trade lock announced (blog.counter-strike.net)	No. Slowed item movement; the OpenID request path was not changed.
2022-05-10	Trade-cancellation endpoints removed from the public Web API (user-detected; no Valve changelog — node-steam-tradeoffer-manager #325)	No. Closed the offer-swap tooling; OpenID authentication was not modified.
2023-12-04	API-key creation now requires mobile confirmation (steamcommunity.com/dev/apikey; no changelog)	No. Protected the key endpoint; the auth hosts documented here were not affected.
2026-09-19 / 09-21	Steam Link Filter state as observed by the authors	No. 14 main domains returned a block in the saved 2026-09-21 recheck — 26 split pairs in the register by 2026-09-22 — while the proxy carrying each login kept running.

Sources: Valve statement of 13 July 2016 (store.steampowered.com/oldnews/22883, archived 2026-09-21) · CSFloat engineering account of the 2017 closure (blog.csfloat.com, archived 2026-09-21) · Link Filter state: linkfilter-recheck-2026-09-21.json.

This finding is falsifiable by a single published instance in which Valve refused an OpenID request because `openid.return_to` pointed to a gambling auth host. No such instance has been located in the public record.

`The two most recent auth-host registrations`

howl.uno was registered 2026-08-11 (RDAP), 41 days before 2026-09-21; howl.gg returned a Link Filter block on 2026-09-18, 2026-09-19 and 2026-09-21. Whether the block preceded the registration is not established.
rbsnin.com was registered 2026-09-18T09:34:52Z (Verisign RDAP) and was observed in Rollbit's Steam login flow on 2026-09-20 via Steam's own login-page notice; rollbit.com returned a Link Filter block on 2026-09-19 and 2026-09-21, rbsnin.com did not.
Each host in the table above is sent to Valve's authentication servers as `openid.realm` on every login attempt.

Full per-route data and Link Filter verdicts: the table in Section 3 above; raw results in linkfilter-recheck-2026-09-21.json and linkfilter-all-results.json.

Methodology — How the Route and Link Filter Counts Were Established

1. Domain resolution

The 2026-09-21 audit resolved 78 of 189 requested platforms: **33 authenticate on their own hostname and 20 on their own subdomain — direct authentication, and none of them are counted as separate-domain routes.** The remaining **25 authenticate through a separate registrable domain**, across 24 distinct hostnames (dota2.net is shared by market.csgo.com and rust.tm): 10 established by live browser capture, 3 by Steam's own login-page notice, 12 by a supplied OpenID URL. The live register (master_registry.json, 2026-09-22) extends that to **44 separate-domain routes**: 26 filter-split pairs (main domain BLOCKED, auth host CLEAN) plus 18 further routes without a main-domain split. Of the 44, **27 carry a per-route evidence file**; the other 17 were collected by hand and are marked `realm_src: user` in the register. Five of those seventeen — csgogem.com, gamdom.com, 12cs.fail, csgolounge.com and dota2lounge.com — were added on 2026-09-22 with a Link Filter capture of both hosts (raw HTML + SHA-256 in linkfilter-2026-09-22.json), so the split itself is evidenced even though the realm is hand-collected; they appear in the table above alongside the evidence-file routes. `tfauth.com` (tf2easy.com) was dropped from the register on 2026-09-22: like arena.fragnet.net, nothing verifiable links it to its origin site. The count is re-derivable from the published auth-route-audit.json (run of 2026-09-21) by one rule: a platform counts only when its observed Steam OpenID host sits on a different registrable domain than the platform itself.

2. Steam Link Filter status

Tested via `steamcommunity.com/linkfilter/?url=https://[domain]`, unauthenticated, on 2026-09-19 and 2026-09-21; raw HTML saved with SHA-256. Status recorded for main domain and auth host separately. A classifier distinguishes the generic "You are leaving Steam" notice (CLEAN) from the "Link Blocked! ... flagged as potentially malicious" page (BLOCKED); a google.com control confirms the two are not conflated. An earlier authenticated variant of this test was discarded after it returned "blocked" for every domain including that control — traced to an invalid session cookie in the probe script, not a real result.

3. Observation of the auth host

Live capture: a Playwright browser navigated to each platform's login flow and the `openid.return_to` hostname was read from the intercepted request. Login-page notice: the hostname was read from Steam's own "*<host> is not affiliated with Steam or Valve*" text, which Steam renders from `openid.realm` (rbsnin.com, sc-auth.net, auth.dota.trade). Supplied URL: a Steam loginform URL provided to the authors; this establishes the request parameters, not a completed login. No login was completed on any platform.

4. Coverage — what was not resolved, and why that matters

Of the 189 platforms, **110 produced no established route** and one was not applicable (189 − 78 − 1). This dossier counts none of them. The breakdown of the 110, from the audit file: 22 bot challenges, 14 timeouts, 12 HTTP errors and 10 navigation errors — the observer could not reach the login flow, though most of these sites open normally in an ordinary browser; 20 showed no Steam login control on the landing page; 16 reached a login flow that could not be resolved to a host; 11 domains did not resolve in DNS; 5 stopped at a consent wall. The register below splits the same 110 differently: the 11 that did not resolve in DNS are listed separately as *Removed · NXDOMAIN*, and the one not-applicable entry joins the rest. 189 platforms audited,

11 removed on a definitive NXDOMAIN from both resolvers, **178 retained** (platform-audit.json, platforms-removed.json). **137 auth domains that the ledger had guessed by naming pattern were deleted from the data on 2026-09-19 — never observed, therefore never evidence.** Three of the guesses were contradicted by supplied OpenID URLs: buff.163.com, gamerpay.gg and csgoluck.com authenticate directly, against guesses of buffauthproxy.163.com, gamerpayredirect.io and lucklogin.app. The removals are listed in the published audit file.
The 25 is a floor, not a ceiling. Among the 78 platforms that did resolve, 25 used a separate domain and 53 did not. Nothing about the unresolved 110 is assumed from that ratio, and no projection from it appears anywhere in this dossier. Each one is resolvable by a person opening the site and pressing "Sign in with Steam": the auth hostname is in the URL of the Steam page that loads.
The point of this section: an independent observer needs a browser and a lot of patience to resolve 189 platforms, and got 78. Valve needs a database query. Every platform that uses "Sign in with Steam" — resolved and unresolved alike — sends `openid.realm` to Valve's authentication endpoint on every login. The gap in this table exists because the authors are outside the system. It does not exist for Valve.
Observed proxy hostnames are in auth-route-audit.json. Domain registration dates from RDAP (Verisign) / IP2WHOIS. Link Filter results in linkfilter-all-results.json.
Analogy for clarity
Imagine a licensed taxi company is told by regulators that it may no longer operate from its registered Main Street address. The company removes the sign from Main Street. That sign removal is documented. However, the same company opens a Side Street address — registered under a different name — and continues operating from there. The regulators operate the central dispatch system that every taxi from both addresses uses. Every ride request shows "pick up from Side Street." The regulators never revoke the Side Street licence. **The removal of the Main Street sign is the only enforcement that occurred. The taxi company never stopped operating.**

Part A — Technical record · Section 4

An endpoint closed. Public tracing lost a key.

Context & source limits
Steam shipped changes that removed public visibility of item Asset IDs and restricted API inventory access. The effect: tracing a specific item by its original Asset ID became impossible from public data. What follows is what was possible before, what stopped being possible after, and what that costs a victim trying to prove where their property went. The date is 2017 according to CSFloat's engineering account; no Valve changelog has been located. The sequence — roughly a year after the July 2016 gambling statement — is the investigative question, not a finding. The item records themselves remain inside Valve's systems; outside investigators lost access to the original-ID chain, while float, seed and paint identifiers allow only partial matching.

The rule Valve applies: Steam Support does not restore items that left your account, and the burden of showing what happened is yours. **The record:** in 2017 Valve closed the endpoint that carried original item IDs. Before it, anyone could follow a stolen skin from the victim's account

into a marketplace bot. After it, nobody outside Valve can. **The proof the victim is asked for is the proof that was switched off** — and it still exists, inside Valve.

The Pre-Blackout Era

Historically, every virtual item generated on Steam possessed a globally unique, immutable Asset ID. Third-party OSINT databases could index these IDs. If a user had an item hijacked, investigators could trace the lineage of that specific asset as it moved from the hijacker's intermediate account into the storage accounts of a marketplace or gambling site.

BEFORE: an item could be followed from the victim's account through intermediate accounts and into a marketplace or casino storage bot, by anyone, using public data.

After the change

According to CSFloat's engineering account, Valve closed the endpoint in 2017 and original item IDs stopped being available to outside parties. No Valve statement of the reason for the change has been located. In the same period, no published action against the commercial bot accounts that moved items at scale has been located either.

Whatever the reason for it, the change severed the public chain of custody. A victim can no longer reproduce the original-ID chain from public data to show that a specific stolen item was liquidated through a specific marketplace or casino. The item records still exist inside Valve's systems; the public, researchers and law enforcement working from public data cannot reach them.

AFTER: tracing a specific item by its original Asset ID is no longer possible from public data. The original-ID chain of custody for an item moved after 2017 exists only inside Valve's infrastructure; no such record has been produced publicly. Float, seed and paint identifiers allow only partial, probabilistic matching.
IEconItems_730
GET `/IEconItems_730/GetPlayerItems/v1/`
Traceable Payload (Pre-Patch)

```
"id": "14892281934",
"original_id": "11829910211",
```

Status: Victim can track item lineage across bot accounts.
Obfuscated Payload (Post-Patch)
Current

```
"id": "HIDDEN_BY_PRIVACY_SETTINGS",
"original_id": "NULL",
```

Status: outside parties can no longer trace item lineage by original Asset ID from public data.
Effect on evidence: after the change, the public data needed to follow a specific item by its original Asset ID from a victim's account into a marketplace or casino bot was no longer available. The internal records still exist at Valve; a victim, researcher or investigator working from public data cannot reproduce the original-ID chain (float, seed and paint identifiers allow only partial matching).

Source: CSFloat engineering account of the 2017 closure of `IEconItems_730/GetPlayerItems` — blog.csfloat.com/how-floatdb-tracks-items (archived 2026-09-21) · the payloads shown are an illustration of the field shape, not captured responses · no Valve changelog for the closure has been located.

One session. More access than the user sees.

Context & source limits
Valve's API-key architecture, as it stood before the 2023 changes, departed from baseline industry standards (OWASP ASVS, NIST SP 800-63B) and is the mechanism described in the automated inventory-theft complaints preserved in the evidence archive (Sections 6–8).

The rule Valve applied: the account holder created the key, accepted the terms, and bears the loss — that is the answer in the archived refusals. **The record:** until December 2023 a stolen session cookie alone could register that key. No password. No Steam Guard. No notification to the person whose account it was. **The user did not create the key, could not see it, and was told he did.** Mobile confirmation was added on 2023-12-04 — about seven years after the 2016 statement and roughly six after the scam panels the archive preserves. Those years were not paid by Valve. They were paid by the accounts emptied in the meantime, a share of them children's.

OWASP ASVS 2.8 / NIST SP 800-63B SEVERITY: CRITICAL

1. Insufficient Step-up Authentication

Steam allowed the generation of highly privileged, long-lived API keys using only a session cookie. No 2FA (Steam Guard) or step-up authentication challenge was required when setting up or modifying a developer API key, so the Steam Guard mobile confirmation — the only second factor Steam offers — did not protect this step. (A hardware second factor was requested in Valve's own tracker in 2016 and the issue is still open: Appendix D, GH-01.)

Status: unpatched before 2023. Allowed a script holding a stolen cookie to register a key without any user interaction.
OWASP A01:2021 / Least Privilege SEVERITY: CRITICAL

2. Lack of Principle of Least Privilege

The Steam Web API lacked any role-based authorisation scopes. A developer API key issued for "read-only" inventory status possessed complete "write" permissions — including the ability to manipulate existing trades, initiate new ones, register webhooks and decline valid pending exchanges.

Status: systemic design defect. One key = full read/write control of the account's inventory and trades.
OWASP A07:2021 / Sessions SEVERITY: HIGH

3. Broken Session Management

Hijacked web sessions originating from server-hosting IP ranges were reported by users to persist. Standard practice is to terminate sessions on geographic anomalies and on password change; user reports collected in the archive describe sessions that remained active after a password change.

Status: reported behaviour (user complaints in the archive). Sessions could generate API keys without re-authentication.
Domain-level blocking was technically feasible ENFORCEMENT FEASIBILITY

4. Domain-Level Blocking of Auth Hosts Was Technically Feasible

Valve already operates a domain list (the Link Filter) and already receives every auth hostname in its own OpenID requests. The two mechanisms are not connected in any way visible from outside: as of 2026-09-22, in 26 pairs the main domain was on the filter while the proxy carrying its login was not.

Connecting them is a small engineering task: read the `openid.realm` hostname from each incoming request, compare it against a list, and refuse or flag the request. The illustration on the right shows the shape of such a routine. Refusing the auth host — rather than only the public landing page — would interrupt the "Sign in with Steam" step that these platforms depend on.

No public evidence shows that Valve runs such a check. The Steam Community Market's combined fee of about 15% applies to sales completed inside the Market; it is not collected on these platforms' external trades.

block_auth_hosts.py ILLUSTRATION
// Read the host Steam already receives — no scanning
def on_openid_request(request):
host = parse_openid_realm(request)
if host in blocked_domains:
refuse(request)
Note: pseudocode for illustration only. Both halves already exist at Valve — the auth hostname arrives in the request, and the domain list is the Link Filter. No public record explains why they are not connected.

`Section 5.1 — The standards were not unpublished`

Valve builds against these rules every day. It did not build to them here.

Steam ships on the App Store and Google Play, sells through the major card processors, and consumes third-party APIs like any other large platform. Each of those relationships carries a published, dated security requirement that Valve must satisfy to keep operating. Set the dates of those requirements against the dates on which Steam's own Web API acquired the same protections. **Nothing below is a private standard, an internal memo or a trade secret: every row is a public document with a publication date.**

Published external security requirements, with their dates, set against the date the Steam Web API acquired the equivalent control

The published standard, and the date it took effect	The Steam Web API on the same question
Scoped authorisationOAuth 2.0 — RFC 6749, October 2012. Section 3.3 defines `scope` so a client receives only the access it asks for. It has been the default of every major platform API since.	**Granular scopes arrived on 16 January 2026.**Before that a single Steam Web API key carried full read and write over the account's trades regardless of why it was issued. **Thirteen years and three months** after the specification that defines the control.
A key is not an authorisationGoogle's own Cloud documentation: "A standard API key doesn't authenticate a principal", and for APIs that create or manage resources, "don't use authorization keys in production."	**The Steam Web API key was exactly that.**A bearer string, issued to an account, sufficient on its own to read the inventory, cancel a pending trade and send a new one. No principal was authenticated at the point of use.
Multi-factor authentication on privileged accessPCI DSS 3.2, requirement 8.3 — mandatory from 1 February 2018 for all non-console administrative and all remote access to the cardholder data environment. Apple then required two-factor authentication of every Developer Program account holder from 27 February 2019: "developers with the Account Holder role in a developer program will need to enable two-factor authentication to sign in."	**A second factor was required to create an API key from 4 December 2023.**Until then a stolen session cookie was enough, with no prompt on the account holder's phone and no notification afterwards. **Four years and nine months** after Apple made Valve itself use a second factor merely to sign in to a developer portal.
Credential lifecycle and revocationTwitch requires of every third-party application: "Your app must validate the OAuth token when it starts and on an hourly basis thereafter", and states that it audits for applications that do not. Its legacy v5 API was retired outright on 28 February 2022 on a published schedule.	**No published key-lifecycle record.**The 2023 change protected the creation endpoint. No Valve statement located with it addresses keys already registered, and no changelog accompanied the change at all. Whether keys created before it were invalidated cannot be established from public data — which is the question a data subject would need answered to know whether a key created on their account years earlier is still live.

`Architectural Benchmark // Token Architecture`

GitHub Fine-Grained Scopes vs Valve Steam Web API

Valve developers manage open-source software on GitHub daily using granular least-privilege tokens. Compare that with the monolithic key issued to 130M Steam players.

GitHub Fine-Grained Token
Used by Valve on GitHub
Fine-grained token with scoped isolation and mandatory lifecycle enforcement.

Repository Access: Selected Repos only (1 repo)
Issue Permissions: Read-only [✓]
Code & Secrets: No access [✕]
Expiration: 30 Days (Mandatory TTL)
Audit Logging: IP, User-Agent & Timestamp
Security Posture: Least-privilege token limits damage to a single read-only resource.
! Valve Steam Web API Key
Issued to 130M Users

Single 32-character master string carrying all-or-nothing trade and inventory authority.

Account Access: FULL ACCOUNT (Monolithic)
Trade Management: Read, Cancel, Decline [!]
Granular Scopes: NONE (Arrived 2026, 13y late)
Expiration: NEVER (Valid indefinitely)
Audit Logging: NONE (Zero IP history for user)
Vulnerability: Stolen key allows silent interception of all outgoing trade offers.

`The standard applied in one direction`

Suppose a vendor Valve depends on — a cloud provider, a payment processor, a CDN — left a credential endpoint without a second factor, and months later Valve's own corporate data left through a key minted at that endpoint. Would Valve accept that the fault lay with whoever clicked the link? The archived refusals preserved in this dossier answer the mirror-image question for the user: the position taken is that the account holder created the key and bears the loss. **The same architecture is described as the vendor's failure in one direction and the user's responsibility in the other.** Which it is, is not a technical question, and it is not one this investigation can settle — it is what a court or a supervisory authority decides.

`Illustration, not evidence — the standard read back the other way`

- A payment processor that let a third-party script mint a full-privilege transaction credential from a browser cookie alone, with no prompt to the account holder.
- An identity provider that closed the hole its tokens were minted through and published nothing about the tokens already minted.
- A bank that answered a disputed transfer by observing that the credential used was registered on the customer's own account, and closed the ticket.

None of these is offered as a finding about any named company. They are the same design decisions, moved to a setting where the supervisory response is well documented — which is the comparison a regulator is being asked to make.

What the record establishes: the controls absent from the Steam Web API were public, dated and, in several cases, conditions Valve had to satisfy to keep shipping its own products. The interval between each standard and the equivalent Steam change is measurable and is set out above. **What it does not establish is why.** No Valve statement of reasons for any of these intervals has been located, and none is assumed here; that record exists inside Valve and has not been published.

Sources, each a public document: OAuth 2.0 — RFC 6749, October 2012 ↗ · Google Cloud — API keys documentation ↗ · PCI DSS 3.2 requirement 8.3 — PCI SSC resource guide ↗ · Apple — Upcoming Two-Factor Authentication Requirement for Account Holders, 20 February 2019 ↗ archived 2025-05-06 ↗ · Twitch — token validation requirement ↗ and the v5 shutdown notice ↗ archived 2025-01-27 ↗. Steam's own dates are those in the update record in this section; the 2023 and 2026 entries are the ones Valve shipped without a changelog. Retrieved 2026-09-22.

Valve's own update record — dated, from public sources

Date	Valve change	Announced?	What it closed	Lag: mechanism public → fix	Source
2026-09-01	Automated Suspicious Chat Flagging	Yes	Dangerous links / patterns in group chats	—	news ↗
2026-01-16	Steamworks Web API granular scopes	Yes	Least-privilege scopes for developer keys	—	announcement ↗
2025-07-15	CS2 Trade Protection & reversal window	Yes	**Nothing.** Not a root-cause security fix. Support-side account recovery access remains untouched. Triggering reversal inflicts an automatic 30-day trade lockout (Skinvault ↗), while cash-trading shock caused a $104M (-25%) 24h market cap plunge (CSMarketCap ↗). In 2026, timers became per-item (Skin.land ↗).	—	FAQ ↗
2025-05-14	Account Security Announcement	Yes	Stealer / session-hijack guidance	—	announcement ↗
2024-10-02	CS2 'The Armory' 7-day hold	Yes	Hold on trade/market for Armory items	—	announcement ↗
2024-09-18	New-device login trade restriction	Yes	2–7 day trade lock on new devices	—	FAQ ↗
2024-02-14	Profile name & avatar change hold	Yes	2–4 h cooldown on trades after rename	—	post ↗

Date	Valve change	Announced?	What it closed	Lag: mechanism public → fix	Source
2023-12-04	Mobile confirmation for API keys	No changelog	Silent cookie-only key registration	≈6 years after the 2017-era panels	dev page ↗
2023-10-24	SMS MFA for game build publications	Yes	Steamworks build publishing	—	announcement ↗
2023-07-12	Custom biography content warning	Yes	Phishing links in bios	—	forum ↗
2023-01-25	Profile {LINK REMOVED} & cooldown	Yes	Links in profile text	—	FAQ ↗
2022-10-24	Login overhaul & cookie truncation	No changelog	Infinite stolen sessions	— (IAuthentication Service token migration)	news ↗
2022-10-12	Mobile App 3.0 QR login	Yes	Session deauthorisation panel	—	news ↗
2022-05-10	Trade-cancellation endpoints removed	No changelog	Offer-swap (cancel & re-send)	≈5 years after the 2017-era panels	issue #325 ↗
2020-05-25	Dota 2 7-day trade lock	Yes	Fast item flipping	—	blog ↗
2018-03-29	CS:GO 7-day trade lock	Yes	Instant bot laundering	≈20 months after the July 2016 statement	blog ↗ archived 2025-02-26 ↗

Sources: the linked Valve posts, help pages and GitHub issues, as dated. Three decisive fixes shipped with no changelog (2022-05, 2022-10, 2023-12) and were detected by users, not announced by Valve — that asymmetry is part of the enforcement record. Lags are computed only where the dossier's own dating (July 2016 statement; 2017-era scam panels) supplies the start point; "—" means no such start point is established here.

Part A — Technical record · Section 6

Interactive Exploit & Hijack Simulator

Context & source limits

A reconstruction of the path from the phishing message to the server-side key registration and the trade swap. Before 2023, a Web API key registered on an account could read its inventory, cancel a pending trade offer and create a new one, and no trade-confirmation screen was

shown to the account holder for any of those actions. That is the absence of least privilege (OWASP A01:2021). The timings in this simulation are illustrative and are not live measurements of the current platform.

Step through the reconstructed hijack. Each phase shows what the account holder sees and, beside it, the call Steam receives at the same moment. **Every one of those calls is correctly authenticated.** Nothing in the sequence needs Steam's authentication to fail — it needs the key it issues to carry no scope (OWASP A01:2021).

What the player sees. What changes behind it.WALKTHROUGH SIMULATOR
01 / THE CHAT LURE**A friend asks to vote**Victim receives a message with a link.
02 / THE LOGIN**A lookalike portal**Victim enters sign-in credentials.
03 / THE ACCESS**Silent Web API creation**Attacker registers a developer key.
04 / THE SWITCH**Legitimate trade swapped**Clone bot duplicates target recipient.
05 / CONFIRMATION**Counterfeit approved**Wrong offer approved on mobile.
The Exploit Completed. Expecting a mobile prompt for their original trade, the victim approves the replacement trade. This is an integrated forensic walkthrough showing how the absence of Least Privilege (OWASP A01:2021) enables automated, sub-second asset hijacking.

The same step, seen from the networkReconstruction of the pre-2023 pattern · illustrative call shapes
VictimApproves the mobile prompt that was expected for the original trade.
AttackerReceives the items at the clone account.
Steam seesA transfer confirmed by the account holder on a registered device.

```
Confirmation genuine — made by the account holder
Recipient the clone bot, not the intended counterparty
The confirmation is authentic. The offer it confirms is not the one the user initiated.
```

The record left behind: a trade the user approved. That is the record Steam Support reads when the complaint arrives, and the reason the archived complaints were closed as user error. The complaints are in the enforcement archive.

Part A — Technical record · Section 7

The endpoints behind the sequence.

Context & source limits
These are the Steam Web API endpoints that the reported hijack scripts used to intercept trades without passing through the browser-side confirmation steps.

Four documented endpoints do the whole job. None of them is a flaw, none needed exploiting — a valid key calls them and Steam answers. **The key is the only thing the attacker had to steal.**

IEconService / GetTradeOffers / v1 POLLING

Used to monitor the account's trade offers. Scripts poll this endpoint repeatedly with the compromised API key; it returns the details of newly created, pending or modified trade offers. Polling intervals are not measured here.

Threat vector: Discloses pending trade offer IDs and the recipient's profile details.
IEconService / CancelTradeOffer / v1 INTERACTION
Used to programmatically invalidate the user's legitimate trade offer. Before 2023 no step-up authentication protected the key, so an automated server could cancel an offer as soon as it was detected, without any prompt to the account holder.

Threat vector: Voids the trade before the account holder completes the mobile confirmation.
ISteamUser / GetPlayerSummaries / v2 RECON
Queried to retrieve the profile name, avatar image URL and level of the legitimate trade recipient. This lets the script dress a prepared clone account to match. No timing is measured here.

Threat vector: Supplies the data needed to impersonate the intended recipient.
/dev/ajaxregisterkey CREATION
Steam's registration endpoint for keys. Historically, any active browser cookie session (`steamLoginSecure`) could register a key without a Steam Guard confirmation on the mobile device, and without any notification to the account holder.

Threat vector: A persistent credential created by a script, unseen by the account holder.

Part A — Technical record · Section 8 · GDPR Article 7

A checked box. Whose action?

Context & source limits
In declining reimbursement, Steam Support replies preserved in the archive take the position that the account holder created the API key and, by checking the box, accepted the terms.

The support response attributes the key to the account holder. The question is whether the record establishes who actually created it.

In the observed API-key hijack pattern, however, the victim never saw or navigated to the API key creation page. The consent field is submitted by a script executing a headless POST with the stolen session cookie.

Under GDPR Article 7 and Article 4(11), consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. The authors' position is that a terms-acceptance field submitted by a hostile script with a stolen cookie, with no page shown to the account holder, cannot meet that definition. Whether it does is for the supervisory authority.

Forensic Payload Analysis: Key Registration
POST https://steamcommunity.com/dev/ajaxregisterkey
// Request Payload (Injected via hijacking script)
{
"agreeToTerms": "agreed", ← machine-injected, no human interaction

"domain": "localhost", ← not validated — any value accepted, including localhost
"sessionid": "8f0d8ef763ab2140bf89de2a"
}
The question for the supervisory authority: where the account holder never clicked the consent field, whether the terms-acceptance recorded against the account meets Article 7's requirement of a freely given, specific, informed and unambiguous indication of the data subject's wishes, and whether Steam Support may rely on it to decline a claim.
Source: request shape of key registration as reconstructed from the public endpoint and from hijack reports preserved in the evidence archive (searchable build of 2026-09-17) · the session identifier shown is a placeholder, not a captured value.

Forensic Autopsy · The Trade Substitution Vector

How Valve Finally Neutralized ”Trade Substitution” — And Why It Took 7 Years of Workarounds

For nearly a decade, the **"API Key Trade Substitution" (or API MitM Scam)** was the most lucrative account theft model on Steam, siphoning hundreds of millions of dollars in skins from unsuspecting players. Valve did not eradicate the exploit by fixing the vulnerable API architecture; instead, Valve spent seven years layering four platform-wide friction barriers that crippled community trade liquidity while leaving the root cause unaddressed.

1. The Mimicry Death

Avatar & Name Cooldown (Feb 2024)

The exploit required sub-second mimicry: the scam bot intercepted an outgoing trade, scraped the recipient's avatar/name via `ISteamUser`, and cloned the profile in 200ms. On 14 February 2024, Valve quietly implemented a mandatory **2-to-4 hour trade cooldown (Error 34)** immediately following any profile name or avatar change. A bot can no longer clone a recipient on the fly without locking itself out of trading.

2. The Economic Death

7-Day CS2 Trade Reversal (Jul 2025)

Valve introduced unilateral **Trade Reversals** for Counter-Strike items. Any traded skin is tagged "Trade Protected" for seven days. If a victim discovers a substitution, they click "Reverse Trade" in Steam Support, and the skin is instantly returned to their inventory while freezing the recipient. Because the 7-day trade lock prevents scammers from moving the item to a cashout site, the theft is rendered unprofitable.

3. The Silent Key Death

Mandatory Mobile Push for API (Dec 2023)

Historically, a stolen session cookie allowed malicious scripts to execute a headless background POST to `/dev/ajaxregisterkey` without notifying the victim. On 4 December 2023, Valve mandated an explicit push confirmation on the Steam Mobile App to generate a Web API key, eliminating silent background key provisioning.

4. In-App Mobile Warnings

Account Age & Name Banners (2022–2024)

Valve revamped the mobile confirmation modal to display the trade partner's **Steam account tenure (creation date)**, Steam level, and an explicit amber warning: *"This user has recently changed their profile name"*, breaking the visual illusion for attentive victims.

The Three Flaws in Valve's Patchwork: Why Scammers Simply Shifted Targets

1. The Game Exclusion Loophole (Dota 2 & TF2)

Trade Reversals were deployed exclusively for Counter-Strike 2. **Dota 2 and Team Fortress 2 items remain completely unprotected** due to crafting and socketing complexities. High-tier items worth thousands of dollars (Dragonclaw Hooks, Golden Baby Roshans, Unusual TF2 burning flames) carry zero reversal window. Scammers simply redirected automated API interception onto Dota 2 and TF2 traders, where Steam Support strictly enforces its 2016 "no item restoration" policy.

2. The "Zombie Key" Reservoir (Zero Expiration)

While Valve added mobile push 2FA to generate *new* keys in December 2023, **Valve never revoked, expired, or purged existing legacy API keys**. Millions of active accounts that generated keys (or had keys silently created by phishing/malware prior to Dec 2023) still carry active credentials with **zero expiration (no TTL) and zero inactivity timeout**. Threat actors maintain massive historical databases of these persistent keys, continuing to poll `IEconService` undisturbed.

3. The Victim Penalty: 30-Day Trading Lockdown

Even in CS2, Valve penalizes the scammed player: clicking "Reverse Trade" in Steam Support automatically inflicts a **mandatory 30-day trade and Community Market ban on the victim's account**. Valve punishes the user with a month-long platform exile as a deterrent against "frivolous" reversals, discouraging victims from reversing trades on lower-value liquid items.

The Core Regulatory Scandal: Seven Years of Workarounds vs. One API Scope

Why did Valve spend seven years inventing trade holds, account cooldowns, and reversible trade locks—disrupting the entire gaming economy and wiping out $104M in market capitalization—instead of implementing the industry-standard fix?

As proven by Valve's official Steamworks release on 16 January 2026 (Announcement #493839547938902179 ↗), Valve already built **Granular Permission Groups (General, Microtransactions, Economy, Sales Data)** and **IP Whitelisting** for corporate Publisher Keys. Valve had the engineering solution in hand for years. A single user-facing checkbox—*"Prevent this Web API key from accessing IEconService (Trade Management)"* or a home IP whitelist—would have eradicated the trade substitution scam in 2018 with zero economic collateral damage. Valve refused to give regular players the protection it engineered for corporate partners.

`Part B — Rules and enforcement record · Section 9`

Their rulebook. The recorded platforms.

Context & source limits
This ledger maps explicit clauses from the **Steam Subscriber Agreement (SSA)** and **Steam Online Conduct (SOC)** guidelines directly against active, large-scale commercial entities.

The rule: no commercial use, no gambling, no bots — and Steam Support quotes those clauses when it refuses to return a victim's items. **The record:** the same clauses, on their face, cover the commercial platforms in this register, which run on Steam identities, Steam bots and Steam transfers. **The clause is enforced against the person who lost the skins and not, on any published record, against the businesses moving them.**

In the archived complaints, Steam Support cites the "No Commercial Use" and "No Automation/Bots" clauses when declining to restore items to victims of API-key fraud. The same clauses apply on their face to the commercial platforms recorded in this dossier, which authenticate through Steam OpenID and move items through automated Steam accounts. No market-wide revenue figure is estimated here (see the enforcement statistics below). What the record shows is the rule applied to individual accounts in the archived cases and no published per-operator enforcement record for the platforms. That asymmetry is what this section documents.

`The central question / selective enforcement`

Rules → Scale → Accountability

One rulebook. Unequal enforcement.

The register shows commercial services using Steam identities, inventories, bots and transfers as operating infrastructure. The SSA prohibits commercial exploitation and automation without permission. The archived complaints show that rule applied to individual accounts, while the public record does not show an equivalent operator-by-operator account for the platforms documented here. Publish the rule, the evidence and the enforcement decision for each one.

189websites in audit scope
44separate-domain routes in the live register — 27 with a published evidence file, 17 manually collected. The 189-website browser audit alone resolved 25 of them; the register adds the hand-collected routes.
12 yr 6 mocsgogem.com blocked in the Link Filter; `api.csgem.com` registered 2014-03-08 and never blocked — one of 26 such pairs as of 2026-09-22
No verified totalmarket-wide revenue estimate excluded

`Steam Online Conduct`

> "...you shall not do, or attempt to do, any of the following on Steam: [...] Engage in commercial activity. Examples of such prohibited behavior include: posting advertisements; running contests; **gambling**; buying or selling Steam accounts; selling content, gift cards, or other items; and begging."

store.steampowered.com/online_conduct ↗ archived 2026-09-21 ↗

SSA § 2.G — Commercial use

> "...[you may not] exploit the Content and Services or any of its parts for any commercial purpose, except as expressly permitted elsewhere in this Agreement..."

Valve's 2016 notices, as reported, invoked the personal, non-commercial licence. No operator has produced a Valve authorisation on the record.
store.steampowered.com/subscriber_agreement ↗ archived 2026-09-18 ↗

Steam Web API Terms of Use

> "You may not use the Steam Web API or Steam Data in any way that violates the Steam Subscriber Agreement."

Third-party skin marketplaces operate through automated accounts consuming the Steam API. The rule text leaves no exception for commercial scale. steamcommunity.com/dev/apiterms ↗ archived 2026-09-21 ↗

SSA § 4.C

Automation

Scripts, bots and non-human interaction are restricted. The ledger records bot trading, account farms and automated routing at commercial scale.

Inspect the records tagged under this clause

SSA § 2.G

Commercial use

Commercial exploitation requires express permission. Compare the documented business models, their scale and any disclosed authorisation or enforcement.

Inspect the records tagged under this clause

SSA § 3.A

VPN & location disguise

Disguising residence through IP proxying can lead to termination. Separate-domain auth hosts require a separate analysis: establish what is disguised and which rule applies.

Inspect the auth-host evidence

Steam Help / URL policy

Link obfuscation

Steam prohibits link shorteners and tools that obscure link destinations. A separate auth domain — `rbsnin.com` in Rollbit's login flow, `auth.dota.trade` in CS.MONEY's — raises the comparable question of whether the destination shown to Steam's OpenID verifier identifies the operating

site.

Valve's URL policy ↗
Rule references: Steam Subscriber Agreement, revision 10 September 2026 archived 2026-09-18 ↗ · Steam Web API Terms of Use archived 2026-09-21 ↗ · Steam URL policy (link obfuscation). Counts describe this dossier's records and tags; they are not a count of adjudicated violations.

The trust deficit

Who reviews the decision when support closes the case?

The preserved complaints describe permanent sanctions, unanswered challenges and refusals to restore stolen items. Test those accounts against the actual ticket history, available remedies and account-access logs. A generic phishing explanation cannot establish who initiated a reset or created an API key.

Read the captured complaints ↗Request the underlying records →Moderator relationship graph →

Part B — Rules and enforcement record · Section 10

An automation API. A rule against automation.

Context & source limits
The question this section puts is how the two are reconciled: which uses of the API are authorised, by whom, and on what published criteria. No count of authorised commercial API users is estimated here, and none is implied by the absence of a published list — the absence is the finding, not a number behind it. The Steam Support messages quoted above are reproduced by the ArchiSteamFarm project in its own FAQ (verified verbatim 2026-09-22); they are not Valve publications, and the accounts they were sent to are not identified.

The rule (SSA § 4.C): no scripts, no bots, no non-human systems on Steam. **The record:** Valve ships a headless REST API whose entire purpose is server-to-server automation, and hands the key to any account. **Users are banned for automation; the automation interface is Valve's own product.** Which commercial uses are authorised has never been published.

The ”Game Developer” Fallacy

Steamworks SDK (Legitimate)
Used by legitimate game studios to integrate achievements, matchmaking, and leaderboards into their game clients. Requires complex C++ integration and official partner onboarding.

Steam Web API (The Loophole)
A headless JSON/REST architecture designed for external web servers. In the hijack pattern documented here it is used to read inventories and manipulate peer-to-peer trades from remote servers; its legitimate uses are not catalogued in this dossier.

Who the key is forAn ordinary Steam user has no in-client need for a Web API key; the key page lives under a developer URL and its documented purpose is external, server-side access. The archived hijack complaints describe victims who did not know the page existed until a key had been registered on their account.

The Automation Contradiction

SSA § 4.C provides: "You may not use any form of scripts, bots, macros, or other non-human-controlled systems ('Automation') to interact with Content and Services on Steam in any manner." Yet the Web API endpoints (like `CancelTradeOffer`) require no human UI and no captcha and bypass the Steam client entirely. The API is designed for server-to-server automation; the rule prohibits automation by users; the boundary between the two is not published.

A server-side position in the trade flow

A Web API key lets a third-party server act on the account's trades without the Steam client. In the hijack pattern, that server sits between the account holder and the trade server.

- → No trade-confirmation screen is shown for the key's actions.
- → Allows background polling (GetTradeOffers).
- → Cancels and re-issues offers without user interaction.

Valve built the interface, prohibited user automation in its rules, and has published no criteria for which commercial uses are authorised.

`Part B — Rules and enforcement record · Section 11`

Ten days demanded. Ten years to account for.

Context & source limits
On 20 July 2016 Valve's general counsel gave gambling operators a 10-day deadline. Ten years later (as of the dossier snapshot, 2026-09-21) at least one platform named in press reports of that notice, CSGOFast, is still operational with a separate-domain auth host. The wording is reconstructed below from press reports of 21 July 2016; the reconstruction is not a scan. The enforcement record the notice implied has not been published. The open letter to the Commission is Section 2.

Read the July 2016 notice beside the later observations. The outstanding demand is an operator-by-operator enforcement record.

`One week earlier — 13 July 2016, in public`

On 13 July 2016 archived 2026-09-21 ↗, Valve described how gambling sites used Steam: OpenID for account identification and automated accounts for trading. Valve stated that using those mechanisms to run a gambling business violated its API and user agreements. **Both the description of the mechanism and the prohibition are in Valve's own dated statement.** On 2026-09-21 the separate-domain auth hosts tested returned no Link Filter block, and Valve has published no per-operator enforcement record.

VALVE CORPORATION

Bellevue, WA

DATE: July 2016 (reported by press 21 July 2016)
FROM: Karl Quackenbush, General Counsel
RE: Cease and desist — commercial use of Steam accounts
NOTE: Reconstruction of reported text; not a scan
"We are aware that you are operating one of the gambling sites listed below. You are using Steam accounts to conduct this business. Under the Steam Subscriber Agreement, Steam and Steam services are licensed for personal, non-commercial use only."

"You should immediately cease and desist further use of your Steam accounts for any commercial purposes. If you fail to do this within ten (10) days, Valve will pursue all available remedies including without limitation terminating your accounts."

Reconstruction of the July 2016 notice text, rendered by the authors from press reports of 21 July 2016
Karl Quackenbush
General Counsel, Valve Corp.
Timeline July 2016 – September 2026
Deadline in the notice:
10 Days
July 2016
Elapsed since the notice:
3,715 Days
Fixed count from 20 July 2016 to the dossier snapshot of 21 September 2026, not a live figure
Published enforcement record:
None
No per-operator account of terminations or blocks located
◀ **Days 0–10** — the deadline, to scale**Day 3715** — the snapshot ▶

1. 20 Jul 2016**Ten-day demand issued***Day 0*
2. 17 Feb 2024**DSA obligations apply***Day 2,768*
3. 25 Feb 2026**NY AG complaint announced***Day 3,507*
4. 21 Sep 2026**Dossier snapshot***Day 3715*

Ten years later, **CSGOFast** — named in press reports of the 2016 notices — is operational: csgofast.com returned a Link Filter block on 2026-09-19 and 2026-09-21, while its auth host `steam-login.authtofast.com` (registered 2026-06-30) did not.

Full dated record of Valve's security changes: Security Timeline → · The Washington record and the enforcement standard: below

What the record shows: the 2016 notice set a 10-day deadline; Valve already operated a domain list (the Link Filter) and received the auth hostnames in its own OpenID requests; no per-operator enforcement record has been published. Community reports describe a 2018 action against a marketplace (SkinJar), but those reports are unverified and are not relied on here.

CSGOFAST / THE SAVED AUTHENTICATION ROUTE

Follow the declared return host.

The saved route record links `csgofast.com` to `steam-login.authtofast.com`. The separate hostname is carried in the Steam OpenID request. It gives investigators a concrete address to compare with Valve's filtering and enforcement records.

Inspect the CSGOFast route and its source ↗ · Compare saved Steam Link Filter results ↗

PUBLIC RECORD / WASHINGTON · 2016 → 2026

Two deadlines. One unanswered enforcement standard.

20 JUL

Valve gives gambling sites 10 days

Its counsel's demand warned that continued commercial use of Steam accounts could lead to termination.

27 SEP

Washington presses Valve

The state's Gambling Commission demanded evidence of steps to stop skin transfers for gambling and set a 14 October response deadline.

17 OCT

Valve rejects the charge

Valve answered after the deadline, disputed that it facilitated gambling, said it had disabled associated accounts, and said it did not want to switch off trading and OpenID for everyone. At least one platform named in press reports of the July notices (CSGOFast) was operating a decade later. Both facts can hold only if the operator replaced the disabled accounts; the record that would show this has not been published. The WSGC should ask Valve to reconcile the two.

2026

The routes observed in September 2026

The route register records 44 platforms authenticating through separate-domain auth hosts, including CSGOFast, using the OpenID and trading mechanisms Valve described in 2016. The enforcement record that would show which operators were cut off has not been produced.

THE COMMISSION'S OWN BRIEFING · 30 JANUARY 2018

Eighteen months after Valve replied, the regulator still called it an intent.

Briefing its own legislature at the HB 2881 public hearing, the Commission described the July 2016 statement in its own words: Valve **"announced its intent to crack down on the use of its platform to facilitate skins gambling."** The same page records what that announcement did to the industry forecast — *"as a result,"* the projected 2020 skin-gambling market was revised

from **$19.7 billion** to **$670 million**, a cut of about 97 per cent, on the strength of the announcement alone. The forecast moved. The per-operator enforcement record that would justify it has still not been published.

The market figures are Narus Advisors / Eilers & Krejcik Gaming estimates reproduced in the Commission's briefing, not Commission findings; the same document puts 2016 skin wagering at about $5 billion, roughly $3 billion of it on casino-style sites. Retrieved 2026-09-22, SHA-256 `c507c9025f93da0aadaf395c4d8882f25973211c318ee8e9b6f18a5b3755e050`.

Valve's public 2016 position and today's observable infrastructure can be put side by side. The question is whether enforcement reached the accounts and routes used by prohibited operators. **A ten-day notice is not evidence that the notice was carried out across the operators it named.** The 2018 OPSkins action is the one documented intervention against a named operator; set against 189 platforms checked and no published per-operator record, one documented action does not show a pattern of enforcement.

Washington Gambling Commission's 2016 notice ↗ archived 2026-05-20 ↗ · Valve's 17 October 2016 response (document copy) ↗ · WSGC briefing to the legislature, 30 January 2018 (local copy, 4 pp.) ↗ · the same file on wsgc.wa.gov ↗ · retrieval record & hash ↗ · Valve's 2018 OPSkins action ↗ archived 2026-03-07 ↗ · Current route audit ↗

`Forensic Longitudinal Audit · 2016 Cease & Desist Targets`

The 10-Day Notice Decade: Forensic Survival Audit of the 23 Named Sites

On 19–20 July 2016, Valve General Counsel Karl Quackenbush issued formal cease-and-desist notices to 23 skin gambling platforms, ordering them to cease commercial use of Steam accounts within **10 days** under threat of account termination and legal action. Over 3,700 days later, an empirical audit reveals the true pattern of enforcement: multiple operators never ceased operations, others ran for up to six years after the deadline, and the multi-billion-dollar ecosystem continued to leverage Valve's OpenID architecture.

5+ LIVE
Defiantly operational in 2026 (CSGOBig, CSGO500, CSGOFast, etc.)
6 YEARS
Longest post-notice run before closure (CSGOatse active through 2022)
$5.01B
2016 skin wagering volume (Narus / Eilers & Krejcik)
200+
Active skin gambling sites operating at market peak

Platform / Domain	July 2016 Notice	Enforcement Outcome & Survival Status	Recorded Verification / Primary Links
CSGOBig csgobig.com	10-Day Notice (Jul 2016)	STILL LIVE IN 2026 Temporarily paused, relaunched; authenticates via letmeinbig.com & csgobiglogin.com	X: @csgobig ↗ · FB: csgobigofficial ↗
CSGO500 csgo500.com / 500.casino	10-Day Notice (Jul 2016)	STILL LIVE IN 2026 Rebranded into 500 Casino (Curaçao license #8048/JAZ2014-037), multi-million monthly turnover	Live Platform (500.casino) ↗
CSGOFast csgofast.com	10-Day Notice (Jul 2016)	STILL LIVE IN 2026 Actively operating roulette, crash, and jackpot via steam-login.authtofast.com	Dossier Auth Audit ↗
CSGOLounge / Dota2Lounge csgolounge.com / dota2lounge.com	10-Day Notice (Jul 2016)	STILL LIVE IN 2026 Pivoted to esports coin wagering and crypto betting; maintained continuous operation	Live Platform ↗
CSGOCasino csgocasino.net / csgocasino.gg	10-Day Notice (Jul 2016)	LIVE VIA SUCCESSOR (2026) Domain redirected; active successor portal operates under csgocasino.gg	Successor Domain ↗
CSGOatse csgoatse.com	10-Day Notice (Jul 2016)	SURVIVED 6 YEARS (ACTIVE TO 2022) Continued full gambling operations for six years following Valve's 10-day ultimatum	X: @CSGOatsecom (Active to 2022) ↗
CSGOSweep csgosweep.com	10-Day Notice (Jul 2016)	SURVIVED TO DEC 2017 Operated publicly for 17 months after deadline	X: CSGOSweep Status Dec 2017 ↗
CSGOWild csgowild.com	10-Day Notice (Jul 2016)	SURVIVED TO DEC 2017 Promoted by major influencers; ran for 1.5 years post-C&D before crypto migration	X: @Wild (Active Dec 2017) ↗
CSGOPot csgopot.com	10-Day Notice (Jul 2016)	SURVIVED TO SEPT 2017 Operated high-stakes jackpot betting 14 months past notice	X: @csgopot (Active Sep 2017) ↗

Platform / Domain	July 2016 Notice	Enforcement Outcome & Survival Status	Recorded Verification / Primary Links
CSGODiamonds csgodiamonds.com	10-Day Notice (Jul 2016)	SURVIVED TO MID 2017 Ran through 2017 despite admitted outcome tampering for sponsored streamers	X: @csgodiamondscom (2017) ↗
CSGOLotto csgolotto.com	10-Day Notice (Jul 2016)	CLOSED JULY 2016 Shut down under public scandal; target of federal FTC consent order	FTC Consent Order (Docket C-4632) ↗
CSGODouble csgodouble.com	10-Day Notice (Jul 2016)	CLOSED JULY 2016 Shut down voluntarily immediately after C&D publication	X: @CSGODouble (Closed Jul 2016) ↗
CSGOMassive csgomassive.com	10-Day Notice (Jul 2016)	CLOSED 2016 Ceased public operations in late 2016	X: @csgo_massive ↗
CSGOStrong csgostrong.com	10-Day Notice (Jul 2016)	CLOSED 2016 Ceased public operations in 2016	FB: csgostrongfree ↗
Skins2 skins2.com	10-Day Notice (Jul 2016)	CLOSED 2016 Ceased public operations in 2016	FB: CSNCOM ↗

The Surviving Titans · 2024-2026 Financial & Traffic Blueprint

From 10-Day Warnings to Offshore Conglomerates: The Multi-Billion-Dollar Turnover

Rather than eliminating skin gambling, Valve's 2016 notices catalyzed an industrial evolution. The surviving operators restructured as offshore corporate entities (Curaçao, Belize, Cyprus), pioneered Peer-to-Peer (P2P) trading to bypass bot bans, and now process over **10 million monthly web visits** and **billions of dollars in annual wagering handle** while continuing to authenticate through Steam:

Platform	Monthly Traffic (Visits)	Estimated Turnover / Volume	Corporate Entity & Jurisdiction	Key Regulatory Actions & Model
CSGOEmpire csgoempire.com	2.3M — 9.0M / mo Avg 6+ min duration; 80% direct	$1.5B — $2.5B Annual Handle >1,000,000 P2P skin trades/mo; $6.4M active liquid order floor	Moonrail Limited B.V. (Curaçao #148182) Payments: JHOLT LTD (Cyprus); Founder: "Monarch" (Ossi Ketola)	Pioneered 0% fee P2P item trading; licensed Curaçao OGL/2024/1183/0869

Platform	Monthly Traffic (Visits)	Estimated Turnover / Volume	Corporate Entity & Jurisdiction	Key Regulatory Actions & Model
CSGORoll csgoroll.com	2.74M — 3.5M / mo Avg 9m 23s duration; 16% bounce rate	$1.0B — $2.0B Annual Handle Est. $100M–$200M annual corporate revenue from house edge	Feral Holdings Limited Headquartered in Belize City, Belize (Reg #171519)	Banned by Australian ACMA (May 2023); sponsored tier-1 team G2 Esports with underage players
500 Casino (CSGO500) 500.casino / csgo500.com	220K — 425K / mo ~105k unique monthly visitors	$100k / week ($5.2M/yr) in Royales High-roller wagering requirement: $400 wager per $1 rakeback	Perfect Storm B.V. (Curaçao #150536) Curaçao Gaming Control Board license OGL/2024/1354/0882	Banned by Swedish Spelinspektionen (Nov 2023) for unlicensed targeting of Swedish players
CSGOBig csgobig.com	~169,600 / mo Avg duration 19m 12s; US primary	Multi-Million Annual Volume Mystery boxes, roulette, and case battles	Operates via auxiliary proxy routing letmeinbig.com (reg 2023) & csgobiglogin.com	Target of July 2016 C&D; relaunched with proxy auth architecture
CSGOFast csgofast.com	~150K — 250K / mo Global multi-language audience	Multi-Million Annual Volume High-velocity roulette and crash games	Offshore operational entities Routes Steam auth via steam-login.authtofast.com	Target of July 2016 C&D; never discontinued operations; active in 2026
CSGOPolygon csgopolygon.com / plg.bet	~300K — 500K / mo CIS and Eastern European dominance	Multi-Million Annual Volume Crypto & skin roulette, match betting	Second-wave target (Oct 2016) Pivoted to cryptocurrency with mirror domain plg.bet	Survived a full decade; continues skin liquidation via third-party APIs

The Second Wave: Why Valve's C&D Targeted 43+ Sites in Total

On 17 October 2016, Valve's legal counsel formally disclosed to the Washington State Gambling Commission that following the initial 23 notices on July 19, Valve had sent cease-and-desist letters to **more than 20 additional skin gambling sites** (bringing the official total above 43). This second wave was necessitated because the initial list inexplicably omitted the largest, most notorious gambling hubs in the world:

- **CSGOJackpot.com:** The historic originator of skin jackpots, which handled hundreds of millions in volume before shuttering under threat of federal indictment.
- **CSGOShuffle.com:** The site at the heart of the July 2016 streaming scandal, where Twitch streamer PhantomL0rd secretly owned 33% of the company and was exposed rigging odds with house funds.

- **The Macro Ecosystem (200+ Operators):** According to industry research by Narus Advisors and Eilers & Krejcik Gaming, over 200 distinct skin gambling sites operated in 2016, generating $5.01 Billion in wagering volume from 3.03 million active players. Valve's 43 letters addressed less than 20% of the active market.

Official Government & Regulatory Investigations on Steam Skin Gambling
The skin gambling phenomenon is documented across multiple formal statutory inquiries, enforcement actions, and government position papers:

1. Washington State Gambling Commission (WSGC) (2016–2018)
Issued formal Cease & Desist demand on 5 Oct 2016; published Legislative Briefing on 30 Jan 2018 documenting that skins are cash equivalents and reporting the $5.0B skin wagering volume.

WSGC Legislative Report PDF (Local Copy) ↗
2. U.S. Federal Trade Commission (FTC) (Sept 2017, Docket C-4632)
First federal regulatory enforcement action involving skin gambling against CSGOLotto owners Trevor Martin and Thomas Cassell for deceptive practices and undisclosed platform control.

FTC Decision & Consent Order ↗
3. UK Gambling Commission (UKGC) Position Paper & Youth Audits
The Commission treats in-game items convertible to cash as money's worth. Its 2018 survey found that 3% of 11–16-year-olds said they had ever bet with in-game items (skins).

UKGC 2018 youth survey ↗
UKGC position on virtual currencies ↗
4. Australian Senate Environment & Communications Inquiry (2018)
Federal Parliamentary report on *"Gaming micro-transactions for chance-based items"*, evaluating Valve's loot box mechanics, secondary market cashouts, and regulatory circumvention.

Parliament of Australia Inquiry ↗

`The outstanding demand`

Publish the enforcement record: which gambling accounts and bots were disabled, which return hosts were restricted, and which commercial services received permission. A public prohibition and a homepage warning do not establish that the underlying operation was stopped.

`Part B — Rules and enforcement record · Section 12`

The hostname is already in the request.

Context & source limits
Valve already maintains a domain list (the Link Filter) and already receives the auth hostname in every OpenID request. The pseudocode below shows the logical shape of connecting the two. No public evidence shows that Valve does so.

Valve already runs a domain blocklist. Valve already receives the login host in every OpenID request. **Nothing needs building — the two have to be joined.** That is a hostname lookup against a list Valve maintains itself. The pseudocode below is an illustration, not Valve's implementation.

forensic_autoban.py
```
# ILLUSTRATIVE PSEUDOCODE — Valve.block_domain() and flag_session_as_mitm() are not real API calls. This demonstrates the logical structure of a mitigation Valve could implement against proxy auth domains, not actual Valve internals.
# Illustration: the logical shape of a check on the incoming OpenID request
def audit_openid_request(request):
blocked_origins = database.get_blacklisted_platforms()
proxy_domain = request.params.get('openid.realm')
target_redirect = request.params.get('openid.return_to')

# Logic: If the proxy routes back to a blocked site, ban the proxy.
for site in blocked_origins:
if site in target_redirect:
Valve.block_domain(proxy_domain)
Valve.flag_session_as_mitm(request.session)
# Result: the login request for that host is refused
```

Observation:
Where a main domain is already on the Link Filter (e.g. howl.gg, blocked 2026-09-18/19/21) and its auth host (howl.uno) appears in the OpenID request from that site's login button, the association is observable to Valve from its own request data. The check is automatable; whether it is run is not.

Documented and reported precedents

Valve has intervened against a third-party operator at least once on the record: in 2018 it revoked OPSkins' access over the ExpressTrade system (Valve's announcement ↗ archived 2026-03-07 ↗). Community reports from 2018 also describe a marketplace (SkinJar) losing access; those reports are unverified and the mechanism is inferred from the outcome, not from a disclosed process.

What the precedent establishes:
Valve can cut off a third-party operator's access when it decides to. CSGOFast, named in press reports of the July 2016 notices, was operating on 2026-09-21 with an auth host registered 2026-06-30 that returned no Link Filter block. Why one operator was cut off and others were not is not explained by any published criteria.

`What a registration date does and does not show`

The registration date of an auth host is a lower bound on when the host could first have appeared in an OpenID request; it does not establish continuous use. `sc-auth.net`, for example, was registered 2019-04-02 (RDAP) and was observed in Skin.Club's Steam login flow in September 2026; what happened between those two dates is not in the public record.

Comparative Audit: API Compliance Standards

Enforcement Dimension	GitHub API Rules	Steam Web API (Valve)
1. Compliance Neutrality	Published, uniform rules. Documented rate limits (e.g. 5,000 calls/hr for authenticated users, 15,000/hr for GitHub Enterprise Cloud organisations) and published acceptable-use policies apply to every account.	No published criteria. Individual accounts are terminated under the automation and commercial-use clauses (archived complaints), while no per-operator enforcement record for commercial platforms has been published.
2. OpenID / Auth Proxy Abuse	GitHub's published policies allow OAuth apps and tokens to be suspended or revoked for abuse, and its documentation describes automatic revocation of exposed tokens (authors' summary of GitHub documentation).	Separate-domain auth hosts observed in Steam OpenID flows (e.g. rbsnin.com, howl.uno, sc-auth.net) returned no Link Filter block on 2026-09-21 while their main domains did.
3. Monetization of Abuse	GitHub takes no transaction fee on items moved by third-party automation; its revenue model is subscriptions and marketplace listings.	Valve sells the case keys that produce the items, and the Community Market charges a combined fee of about 15% on sales completed inside the Market. No figure for revenue attributable to third-party platforms is estimated here.
4. Evasion Loop Lifespans	Suspended OAuth client IDs stop working platform-wide at suspension; the documentation does not publish a time-to-action figure and none is assumed here.	Separate-domain auth hosts with registration dates from 2011 to September 2026 returned no Link Filter block in the checks of 2026-09-19 and 2026-09-21. Registration date is a lower bound on possible use, not proof of continuous use.

Sources: GitHub column — GitHub's published API rate-limit and platform-policy documentation (authors' summary, not quoted) · Steam column — Link Filter checks of 2026-09-19 and 2026-09-21 (linkfilter-recheck-2026-09-21.json), RDAP registry (domain-registration.json) and the archived support complaints (evidence archive).

Part B — Rules and enforcement record · Section 13

The off-Steam price gap

The item sits in a Steam inventory; the sale happens elsewhere. A Factory New AWP Dragon Lore had **62 live offers on CSFloat**; the cheapest asked **$10,623.95**. Steam's own market cannot display an asking price above approximately $1,800. To sell for the observed higher price, an owner needs an off-Steam buyer or marketplace. The item and its transfer still depend on Steam.

Context & source limits

Three different counts appear in this section and they are not interchangeable. **245** is the number of CS2 item-name categories whose cheapest active offer exceeded $1,800 on CSFloat alone, 20 September 2026. **241** is that same set minus the four categories pinned at CSFloat's $100,000 ceiling, which is the panel the $13.63M floor is calculated on. **248** is a different snapshot: categories priced above the cap by two or more of five marketplaces on 23 September 2026. The marketplaces overlap, so counts from different venues must never be added. Every figure here is an asking price, not a completed sale, and none of it is revenue, turnover or profit — for Valve or for anyone else. PriceEmpire's listed values are rounded estimates published by that site, and its Steam card covers items from other Steam games, so the scopes across the comparison are not identical.

One item. Two price systems.FOLLOW THE RECORD
STEAM**About $1,800**Published Community Market listing cap
SAVED CATALOGUE**$10,623.95**Factory New AWP Dragon Lore floor ask
THE DEPENDENCY**Still a Steam item**The inventory and transfer remain on Steam
At that ask, the seller needs an off-Steam venue or buyer. The item still depends on Steam's inventory and transfer system.

01 / ITEM**Valve game inventory**CS2 or Dota 2 item held in Steam
02 / CEILING**About $1,800 on Steam**Maximum price for one Market listing
03 / OUTSIDE ASK**$10,623.95 for Dragon Lore**Cheapest CSFloat offer in the dated snapshot
04 / DELIVERY**Steam remains in the chain**Ownership and item transfer rely on its system
245 CS2 categories on CSFloat.166 CS2 and 3 Dota 2 categories on Skinport.
Each figure counts item-name categories whose cheapest active offer was strictly above $1,800 on 20 September 2026. The marketplaces overlap; their counts must not be added. An offer is not a completed sale.

Inspect the item-level register →
DIRECT CSFLOAT API / DATED SNAPSHOT**$13.63M**
Minimum aggregate asking value in **241 item categories** and **3,395 active offers**. Calculated as each category's cheapest ask × its offer count. Four categories pinned at CSFloat's $100,000 ceiling are excluded from this conservative panel.

What the dollar figure shows

These offers represent at least **$13,631,888.25** in posted asking prices for this limited CSFloat subset. Including the four ceiling-priced categories produces **$14,231,888.25**. This is a *floor on active asks*, not completed sales, cash turnover, profit or the entire CS2 market.

Recalculate from the 245-row CSFloat snapshot ↗

PRICEEMPIRE / LISTED VALUE**Steam: #15 of 39**

Many venues list more dollar value than Steam.

UUSkins
$133.8M
YouPin898
$127.5M
Buff.163
$104M
Moon.Market
$100.3M
White.Market
$89.6M
Buff.Market
$86.7M
Steam
$31M
The six largest displayed values and Steam. PriceEmpire rounds these figures; Steam shows **$31M**. Fourteen listed venues rank ahead of it by the displayed dollar values.

PRICEEMPIRE / OFFER COUNT**Steam: #1 of 39**

Steam still leads in number of offers.

Steam
32.2M
YouPin898
5.9M
C5Game
4.6M
HaloSkins
4.4M
Skinport
3.8M
Steam shows **32.2M** offers. Number of offers and total asking value answer different questions; many low-priced listings can dominate the count.

Source: PriceEmpire's public comparison ↗ archived 2026-09-21 ↗, captured 2026-09-20 19:03 UTC; dated 39-row extraction ↗. Its figures are rounded estimates, and inventory can overlap across sites. Steam's card also describes items from other Steam games, so the scopes are not identical. Listed value measures asking prices, not sales or revenue.

42
ANOTHER SOURCE / STEAMANALYST

The commercial ecosystem is in plain sight.

SteamAnalyst's marketplace directory archived 2026-07-19 ↗ lists 42 third-party CS2 marketplaces alongside Steam, with recent price data for 32 of the 43 entries. PriceEmpire lists 39 marketplaces under its own inclusion criteria. Named businesses, public offers, visible prices: this economy is open to inspection.

THE CEILING IS THE MECHANISM: THE SALE LEAVES STEAM, THE ITEM DOES NOT.
Across five marketplaces captured in one licensed snapshot, **248 CS2 item categories are independently priced above Steam's approximately $1,800 listing ceiling by two or more of them — and every single one is absent from Steam**. The same snapshot banded the whole catalogue by price: Valve's market carries 95.3% of the item categories below its cap and 1.9% of those above it. The collapse does not track falling demand; it lands exactly on the published rule. Selling at those prices requires an outside buyer or marketplace, while Steam still controls the inventory and the transfer — the business leaves Valve's checkout and the delivery stays on Valve's infrastructure.

Steam Market FAQ ↗archived 2026-09-21 ↗Steam Subscriber Agreement ↗archived 2026-09-21 ↗Five-marketplace atlas dataset ↗Provenance manifest ↗Earlier CSFloat snapshot ↗Skinport snapshot ↗PriceEmpire ↗ archived 2026-09-21 ↗SteamAnalyst ↗ archived 2026-07-19 ↗Price-gap register ↗Price-ladder atlas ↗

Part C — Legal frameworks

Part C — Legal frameworks · Section 14 · Personnel access

Who can reset the safeguards?

Context & source limits
Account security also depends on the people who can recover an account, inspect private records or reset its safeguards. The investigation must follow those privileged actions as closely as it follows API abuse.

Account recovery hands a support agent the power to move an account away from its owner. **Valve has confirmed in writing, twice — February 2023 and November 2025 — that this power was used to hand accounts to the wrong people.** Thirty-three months apart, through the same channel. Below: what that access is worth, six sourced cases, and the log Valve holds for every one of them and has produced to nobody.

Preserved testimony / 9 May 2025

A recovery ticket that disabled the account's security, and a reported $10,000 loss

A user in the collected support archive reports that Steam Support reset the password and disabled account protection after another person submitted a recovery ticket. The author says the account had been inactive for years, held items since 2016–2017 and had Steam Guard, a linked phone and stored recovery codes.

> "Steam Support still gave someone else access to my account."

First-person allegation, preserved in `steam_support_tickets_MEGA.json`, record 110. Read the complete captured post ↗

This is not one user's bad luck. The same door — a help request that moves an account to whoever supplies the older data — is the documented way in for every case in the ledger below, and Valve has twice put that in writing.

The owner cannot win that argument. Recovery asks for the first CD key, the first email, the first card, the first phone number. Those facts are in Valve's database, and support-side access reads them — reported as reaching back fifteen years. A person who has a copy of your file will always produce more of your history than you can. Targets were picked to fit: dormant for years, high-value, and often bought second-hand, so the holder never knew the original key. Afterwards the accounts were deleted outright, breaking the item-history trail the community uses to trace a skin — a deletion an ordinary user cannot perform without the standard waiting period.

`Least privilege / OWASP A01`

Recovery privileges should be limited to the task, independently reviewed and logged. Audit who could reset credentials, remove Steam Guard, read billing records or export account data. OWASP access-control guidance ↗ archived 2026-09-20 ↗

`Broad support access`

Access-scope risk

Beyond the inventory.

If broad support access is abused, private telemetry can become a tool for profiling, targeted phishing and surveillance. Potential victims include ordinary users, military personnel, public figures and their families. This is a threat model; the exact permissions require access-control records.

01 IP history & location
IP logs can expose network history and approximate location. They do not, by themselves, establish precise physical movements.

02 Device fingerprinting
Device identifiers, where collected and accessible, can connect sessions and accounts.

03 Activity telemetry
Login timestamps and session records can reveal routines, including activity invisible on a public profile.

04 Communications & contacts
Access to retained messages or contact information would increase the scope for profiling and social engineering.

05 Identity unmasking

Original email, phone and payment records can connect a pseudonymous account to a person.

06 Data resale & accountability
Exported target lists could support targeted scams. Establish the actor, access location, recipients and transfers; location alone establishes neither access nor legal immunity.

Valve describes IP logging, device information, payment records and third-party support providers in its Privacy Policy §§ 3, 5.2 archived 2026-09-21 ↗. The policy authorises third-party support access — the audit trail that would show which contractor accessed which category, when, and under what authorisation has not been disclosed.

Section 14.1 · the register · June 2022 → November 2025 · every figure sourced

Valve admitted the door twice, thirty-three months apart. It never closed.

Six reported cases in which accounts were taken through Steam's own help-request channel, or through the credentials that channel protects. Each amount is the figure the cited source published, and each source is named. Two of the six were made whole. The difference between them and the rest was not what happened — it was who was watching.

Valve, in writing — February 2023“"The items in question were removed from your account because they were received from an account that was compromised through a support help request, for which the CS:GO team takes responsibility. We have reversed the trades and removed them from any account which received them."”*Steam Support reply to a recipient of HFB's items, reproduced by Dexerto, 21 February 2023 ↗ archived 2025-08-18 ↗*
Valve, in writing again — November 2025 · 33 months later“"A support technician that handled the help request failed to follow our process which resulted in your account restored to someone else. I apologize for this error."”*Steam Support reply to Hawkeye337, quoted in Dexerto, 14 November 2025 ↗*

1. 21 Jun 2022
   HFB — the largest inventory in the game$2,000,000+ *· raised to $3,000,000+ in the February 2023 follow-up*
   Seven Souvenir AWP Dragon Lores and the #1 Blue Gem Karambit, that knife alone valued at about **$1.26 million**. The account had been dormant three years with the mobile authenticator still active; the email and password were changed anyway, through the support recovery route.

   The money left before the items did. A reported **$200,000+** of sale proceeds was already withdrawn through market.csgo.com — a marketplace that settles in cash and crypto. Reversing a trade returns a skin. It does not return the cash somebody already banked.

   And the fix broke. One buyer moved his Souvenir Dragon Lore into an in-game Storage Unit. Valve's rollback script could not see inside its own container, so it issued the owner a fresh copy and left the hidden one standing — Valve duplicated a **$130,000** item while trying to undo a theft. It was caught by matching item IDs and community reporting, and deleted a month later, in July 2022. The buyer was refunded by BUFF, not by Valve. Emergency remediation this brittle is not a control; it is what a platform does when it has no control.

Dexerto, 21 Jun 2022 ↗ archived 2022-07-02 ↗ · Kaspersky ↗ · cash-out figure per Esportfire, 22 Jun 2022 ↗ archived 2026-05-15 ↗, attributed there to multiple Twitter sources · duplication and deletion per Esportsbetting, 14 Jul 2022 ↗

Restored *Trades reversed. Items pulled back out of the inventories of people who had paid full price for them.*

2. 14 Aug 2022
   CS.Money — the platform's own bots $6,300,000 · *19,000+ skins · first estimate $1.6M*
   Attackers took the mobile-authenticator files of the marketplace's trading bots and emptied them, then sent part of the haul to well-known traders to blur the trail. Community researchers mapped **55 attacker accounts within hours** and published them.

   Valve reversed nothing. The reason given was that a third-party site sits outside Steam — the same Steam whose inventory, trade API and account system the theft ran on end to end.

   Esportfire, 14 Aug 2022 ↗ archived 2025-11-15 ↗

   Refused *No reversal. Loss stayed with the platform and its users.*

3. Reported
   21 Feb 2023
   Qkss — same door, same actor $1,000,000+
   Reported as taken the same way HFB was, by the same actor, through the same support help request. HFB was made whole eight months earlier. Qkss was not.

   One route. Two answers. Nothing in the published record distinguishes the two cases except the size of the audience.

   Dexerto, 21 Feb 2023 ↗ archived 2025-08-18 ↗

   Refused *Not restored.*

4. Reported
   Feb 2023
   The insider trade itself — a year of it ≈ $320,000 · *proceeds over roughly one year, not an inventory valuation*
   Support-side access reached account history up to **15 years old** — the first CD key, the first email, the first card. That is exactly the evidence the recovery process asks for, which is why the person holding the database always wins the argument against the person holding the account.

   Blogger Mzkshow exposed how insider operator "Steam Help" and collaborator "Alexander" targeted dormant accounts holding over $100k in skins. One stolen M4A4 Howl carrying iBUYPOWER and Titan Katowice 2014 holos sold for **$35,000** and ended up with NAVI's Valerii "b1t" Vakhovskyi, who had no way of knowing. After Valve intervened, the contractor dismissed its entire Steam support desk.

   VKPlay ↗ · Lis-Skins ↗ · Escorenews (RU) ↗ · Dexerto (EN) ↗

   No register *Valve has never published how many accounts this touched, or told the people it touched.*

5. Reported
   2 Dec 2024
   "Matvey" — after the sackings$13,000
   Recovery was granted to someone who supplied account data the owner himself could not match. Two years after the contractor cleared out its Steam support desk, the same route produced the same result.

   Preserved post, 2 Dec 2024 ↗ archived 2025-08-05 ↗ · source rows & hashes ↓

   Refused*Not restored.*
6. 13 Nov 2025
   Hawkeye337 (Mark Spurlock) — and the second admission≈ $300,000–$500,000 · *full Katowice 2014 holo collection*
   The attacker demanded **1 bitcoin** and began scraping the collection onto Negevs to destroy it. Steam Support's written reply is the second admission above: a technician handled the help request, did not follow the process, and gave the account to someone else.

   What produced the fix was the feed. Hours after the posts tagging Valve went up on X, the account was taken back and every sticker restored. Qkss did not have that audience.

   Skin.club ↗ · Dexerto ↗ · Esportfire ↗ archived 2025-12-17 ↗

   Restored*Reversed within hours of the story trending.*

What the ledger says that no single case does.

The route never closed. The first admission is dated February 2023 and the second November 2025 — **thirty-three months apart**, with the contractor's mass dismissal, a documented recurrence and a $6.3 million platform breach in between. Counting from the first theft in this ledger, the channel stayed open for **three years and five months**. Whatever was fixed in 2023, the help request still moved an account to the wrong person in November 2025 — Valve's own sentence.

Restitution tracked attention, not harm. Restored: the biggest inventory in the game, and the collector whose thread trended. Refused: $1,000,000, $6,300,000, $13,000. Valve has never published the rule it applies, because a published rule would have to explain those three.

Nobody was told. Not the users whose account histories were read out of the database, not a supervisory authority, not the market that bought the items in good faith and had them clawed back. There is no breach notice, no incident report, no count of affected accounts — **and the proceeds left as money**, through marketplaces that pay in cash and crypto. A trade reversal cannot follow money out of Steam.

Valve holds the support audit trail, the recovery-ticket log and the transaction record for every line above. None of it has been produced. Ask for your own copy →

The NDA question

Confidentiality must come with technical accountability.

Compare confidentiality agreements with actual permissions, export controls, reset approvals and access logs. A canned response cannot resolve an allegation that the recovery process itself was abused.

GDPR Articles 28, 32–34

Art. 33 gives a controller 72 hours to notify the supervisory authority of a personal-data breach; Art. 34 requires telling the affected people when the risk to them is high. Valve has confirmed in writing, twice, that its support channel handed accounts to the wrong people — account history, billing records and all. **No notification under either article has been published, and no affected user has reported receiving one.** Read the regulation ↗ archived 2026-09-20 ↗

Include support access in your request →

Additional reported case · October 2026

The reset request, and the later objection.

A ticket image published on 13 October records a request for a CD key, a later reassessment and removal of the mobile authenticator, followed by a message disputing the request. The poster identifies the earlier requester as an attacker. The image gives a sequence to audit; it does not establish who submitted the first request or what checks took place outside the exchange.

Read the ticket sequence and full image →
Search the expanded support collection →

9,051 A+B collection rows
2,961 collector Tier A records
5,727 separate leads, excluded from the total
Collected 17 October 2026. The source register distinguishes reported outcomes, quotations, policy pages and repeated sources. Its row counts are not a count of independent victims.

Part C — Legal frameworks · Section 15 · Commercial scale

Follow the money. Separate the transactions.

Context & source limits
The commercial-use question becomes sharper when the money flows are separated. Third-party item transfers, Valve's primary sales and external cash-outs are different transactions.

The item is Valve's. The inventory is Valve's. The transfer runs on Valve's servers. **Only the payment happens somewhere else** — which is the step that decides whether anyone is a money transmitter, and the one step Valve does not operate.

The revenue mechanism

Where the money actually moves.

Three paths / one item economy

1. 01 / Account**User inventory**
   Items held on Steam
2. 02 / Transfer**P2P trade**
   User ↔ bot or user ↔ user
3. 03 / Settlement**External platform**
   Site balance or payment off Steam

CirculationThe economic engine extends beyond a transfer fee
Steam supplies the inventory and transfer infrastructure used by outside markets. The investigation's economic argument is that resale liquidity and repeated demand sustain spending on cases, keys and replacement items, with fees on subsequent Community Market sales. A direct P2P transfer carries no Community Market commission; that accounting fact does not settle the wider benefit. Valve retains control over account access and trading restrictions throughout.

1. 01 / Secondary demand**Liquidity & resale value**
   External trading and gambling demand
2. 02 / Primary spending**Keys, cases & capsules**
   Purchases from Valve where offered
3. 03 / Revenue**Primary-sale income**
   Plus fees on actual Market sales

5% + 10%Steam + CS2 fee on Community Market sales
The investigation's economic inference: liquid resale markets can encourage spending on new items. The familiar 15% combines Market fee rates, subject to minimums and rounding; it is not a levy on every external trade.

Valve's Community Market fee schedule ↗ archived 2026-09-21 ↗. On 25 February 2026 the New York Attorney General filed an action archived 2026-09-01 ↗ alleging that paid loot boxes are connected to external cash resale and gambling harm — the same connection this dossier documents from the technical-infrastructure side. That complaint is an allegation, not a finding; it is cited here because a state law-enforcement agency has put to Valve a question adjacent to the one this dossier asks: where is the enforcement record that matches the public declarations?

1. 01 / Entry**Crypto deposit**
   External service and wallet records
2. 02 / Conversion**Balance → skins**
   Items delivered through Steam trades

3. 03 / Exit**External fiat sale**
   Seller, buyer and payout provider

KYC?Identify the control at every handoff
This is the route to investigate, not a native Steam API cash-conversion service. Document identity checks, custody, transaction IDs and payout recipients at each external operator before asserting a no-KYC cash-out.

United States / Bank Secrecy Act

Classify the activity, then the obligation.

FinCEN assesses money transmission by what a business does. Accepting and transmitting convertible virtual currency can trigger money-services obligations, subject to the applicable definitions and exceptions. Valve's Steam Wallet accepts funds and converts them to in-game items; those items are then liquidated through third-party operators for real currency. The item and its transfer run on Valve's infrastructure; the cash-out does not, and whether any part of that cycle meets the money-transmission definitions is a classification question for FinCEN, not a conclusion drawn here.

FinCEN FIN-2019-G001, §§ 1–2, 5.1 ↗ archived 2025-07-11 ↗

European Union / money laundering

Trace proceeds, knowledge and assistance.

Directive (EU) 2018/1673 covers intentional laundering and participation involving criminal proceeds. The investigative question is what Valve knew about the operators using its trading and OpenID infrastructure after 13 July 2016, when it publicly described that use, and what it did about them. Valve has published no per-operator enforcement record; that record, not this dossier, would answer the question.

EU criminal-law framework ↗

AMLD6 terminology: the criminal-law directive above is distinct from Directive (EU) 2024/1640, also called AMLD6. The latter has a general transposition deadline of 10 July 2027, with specified exceptions. Article 78 ↗ archived 2026-08-30 ↗

Part C — Legal frameworks · Section 16 · Notice, response, responsibility

The Digital Services Act: put knowledge on the record

Context & source limits
Two elements of an Article 16 notice sit with the submitter rather than with this dossier: the submitter's own details and a statement of good faith that the information is accurate. Everything else the Article requires — the substantiated explanation and the exact electronic location — is set out in Section 3 and in the route register, with saved responses and hashes, so

that any party can lodge it. Two further limits on the law itself: losing the hosting exemption does not by itself establish liability under any other law, and the 6% in Article 52(3) is a statutory ceiling, not an assessed penalty against Valve.

Under the DSA a hosting provider keeps its liability shield only until it has specific knowledge and fails to act. **This dossier is that notice.** It names the hosts, the dates, the saved responses and the hashes. From publication the question is no longer whether Valve knew — it is what Valve did next.

01

`July 2016 / the dossier exhibit`

A ten-day demand.

The notice reconstructed above is the historical starting point for the investigation's enforcement comparison.

02

`17 February 2024 / general application`

The DSA time window.

Separate historical conduct from conduct during the period when the relevant DSA obligations apply.

03

`Ten years / original dossier snapshot`

Duration needs a notice trail.

The elapsed time since July 2016 (see Section 11) is a dossier metric. It is not ten years of established DSA violations. Link each notice to a specific item, applicable law, delivery evidence and response.

`Article 52(3) / statutory ceiling`

6%

of annual worldwide turnover

Maximum fine for a breach of DSA obligations, using the provider's preceding financial year. This is a legal ceiling, not an assessed penalty against Valve.

`Articles 6, 8 & 16 / the legal test`

For relevant hosting services, specific knowledge and failure to act expeditiously can remove the hosting exemption. A sufficiently precise notice can establish knowledge of the particular content. The DSA imposes no general monitoring duty; loss of the exemption does not itself establish liability under another law.

DSA: Articles 6, 8, 16, 52, 53, 93 and recital 17 ↗ archived 2026-09-20 ↗

Review preserved complaints ↗Build the account timeline →Full legal & economic analysis →

Minors: a Steam login is not an age check

Context & source limits
No minor's data appears anywhere in this dossier and none was collected: the authors did not register on, deposit at, or complete a login to any platform named. Anyone building on this section should keep evidence involving a child private and redact identifying details from public exhibits. COPPA is cited here as a children's privacy law with its own scope conditions — audience, actual knowledge, personal data collected — and not as a general gambling-age rule; the 2026 New York complaint is an allegation by a state authority, not a finding.

"Sign in with Steam" proves an account exists. **It proves nothing about age** — and on these sites it is the only gate between a child and a deposit. Read it with Section 3.1: inside the Steam client the warning a browser would show never fires, so the child never sees one.

What Steam OpenID provides

Account identity
A verified SteamID used to log in or link an account.

What the operator must establish

Eligibility to participate
Age, jurisdiction and any required identity checks.

Technical basis: Steamworks OpenID documentation ↗ archived 2026-09-21 ↗. The documented identity assertion is not a certification that the user may legally gamble.

COPPA / children under 13

Identify the operator and the data.

COPPA applies to covered child-directed services and services with actual knowledge that they collect personal information from children under 13. It is a children's privacy law, not a universal gambling-age rule. Establish the audience, personal data collected, knowledge and parental-consent process.

FTC: COPPA requirements ↗ archived 2026-09-21 ↗

The evidence to preserve

Record the journey from login to deposit.

Preserve the site's age gate, registration wording, eligibility terms, payment flow and complaint history. Assess each operator separately. Keep any evidence involving a child private and redact identifying details from public exhibits.

A related public enforcement record is the 2026 New York complaint announcement archived 2026-09-01 ↗, which alleges harm to young users from paid loot boxes. It is not a COPPA finding.

Part C — Legal frameworks · Section 18 · GDPR Article 15 request

The request. The reply. The missing comparison.

He asked for four things, one of them the log that would name whoever put an API key on his account. **Three days later the ticket was closed with a link to a page that holds none of them** — and the sentence used to close it is contradicted by Valve's own lawyers.

Whose account this is · Provenance & Limits

These screenshots are not PhishDestroy's. They come from an ordinary Steam account holder — one respondent to a short survey run by this project, who filed the request himself and supplied the captures. The account is his, the ticket is his, and the correspondence is between him and Steam Support. This project did not submit the request, holds no account on the platform, and is not a party to this ticket.

On 16 September 2026 he filed a GDPR/CCPA Article 15 subject access request asking specifically for API-key registration logs, login history with IPs, device authorisation history and trade history. On 17 September agent "Logen" referred him to the self-service Account Data page. On 18 September he stated that the requested categories were not on that page and asked for escalation to the Privacy Team or DPO. On 19 September agent "Kal" closed the ticket with the same referral. Both screenshots are preserved below (requester e-mail redacted; SHA-256 in `steam_tos_assets/screenshot-manifest.json`).

He is a fitting requester for an ordinary reason: **his account carries a Steam Web API key he did not create, registered to** `localhost`. **When it was created is not known** — not to him, and not from anything Valve has made available to him, because the single record that would date it is the API-key registration log, which is exactly the category the closure withheld. The key is not new: it predates his awareness of it by an interval he cannot measure, for the same reason.

Other account holders are filing the same request. Any reply that arrives will be added here on the same terms as these two — ticket number, capture date, SHA-256, requester redacted — whether it supplies the categories or refuses them.

This project takes no position on why the ticket was closed. No reason was stated in it, and none is inferred here.

The request. The response. The comparison.FOLLOW THE RECORD

THE REQUEST**Specific categories**API-key, login, device and trade records

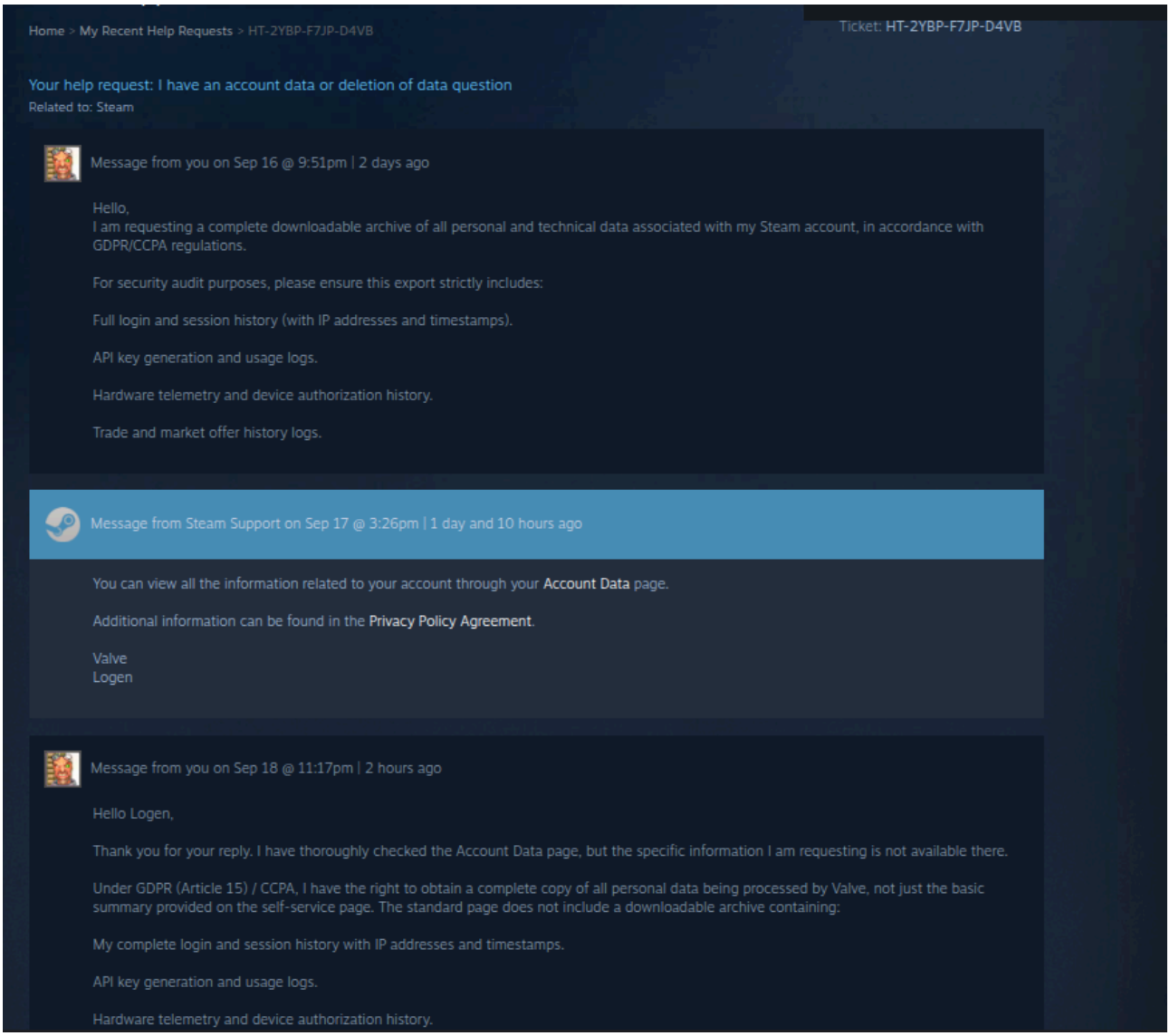
THE RESPONSE**Account Data reference**Inspect the support exchange

THE TEST**What was supplied?**Compare each requested category

He asked for four named categories. The Account Data page he was referred to is Valve's own self-service export, and this project cannot enumerate its contents for someone else's account — so no full category-by-category comparison is published here. What is on the record is his

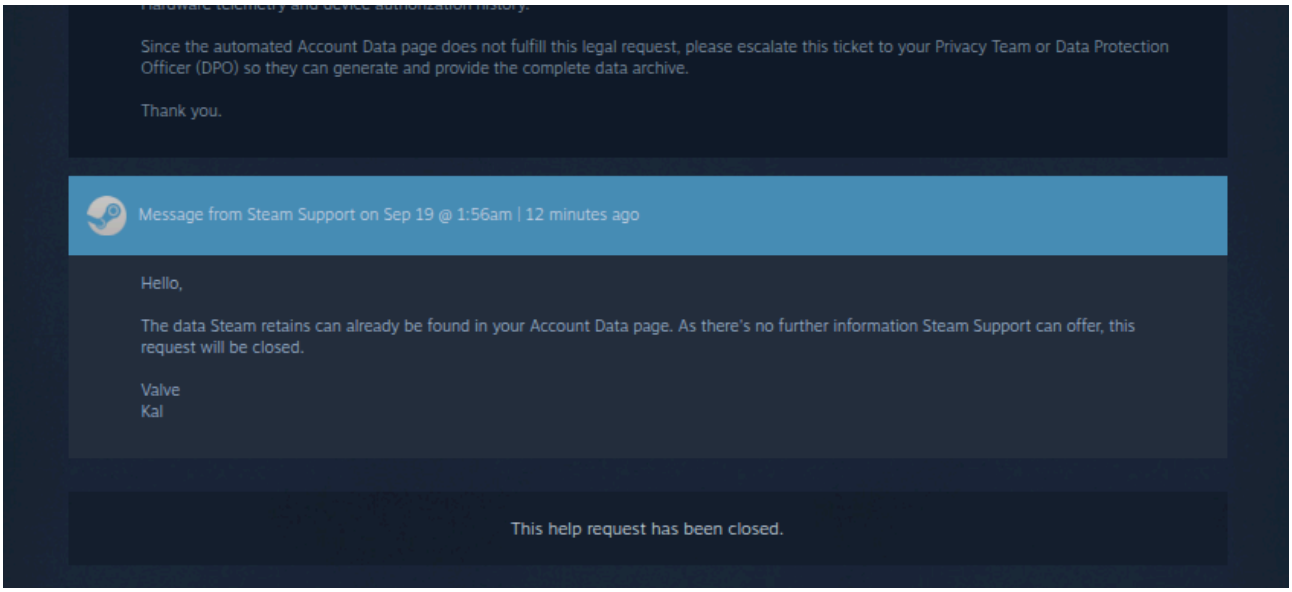
statement of 18 September that the categories were not there, and the closure of 19 September that repeated the referral without addressing them.

Screen 1/2 — Request (16 Sep) and first reply, agent "Logen" (17 Sep)



Source: help.steampowered.com, ticket HT-2YBP-F7JP-D4VB · captured 16–17 Sep 2026 · requester e-mail redacted 2026-09-21 · File: gdpr-ticket-1.png · SHA-256 `da940c731ab9869d226e9d06ccc8a1b393738766b7b0c445a56662623e025a66` (screenshot-manifest.json).

Screen 2/2 — Escalation request (18 Sep) and closure, agent "Kal" (19 Sep)



Source: help.steampowered.com, ticket HT-2YBP-F7JP-D4VB · captured 18–19 Sep 2026 · File: gdpr-ticket-2.png · SHA-256 `44844ea7b251f7fd7d79f87ee1578a846606a97b9659d3a53b322120c422219b` (screenshot-manifest.json).

Closing response, 19 Sep (verbatim):
"The data Steam retains can already be found in your Account Data page. As there's no further information Steam Support can offer, **this request will be closed.**"
No data supplied · no legal basis for refusal stated · no escalation outcome shown
That sentence is false, and Valve's own lawyers prove it. Counsel's letter of 1 October 2025, paragraph 1.9, describes device-level correlation linking one device to dozens of accounts (Appendix A). The same response carried 830 pages of retained records (Appendix B). None of it is on the Account Data page.
Why this account asked for the API-key log
He did not pick those four categories at random. The `localhost` key on his account is **the mark of a script, not of a person typing a real domain into the developer page** (Section 5, Section 6). The one record that shows who created it and from where is the API-key registration log. That was the first thing he asked for. That is what the closure withheld.

Source: the account holder, during this project's survey. The ticket screenshots above are hashed; the key page is not published.

Assessment · PhishDestroy
Closing a ticket with the question still open is not an accident here. It is the normal outcome. We hold 16,319 preserved complaint and support records and 354 de-duplicated support exchanges drawn from them. This ticket is one dated, fully captured example of the shape they take.

Support Ticket — Preserved HT-2YBP-F7JP-D4VB
Request type GDPR Article 15 DSAR
Ticket status CLOSED 19 SEP 2026 — NO DATA SUPPLIED
Agents in the exchange "Logen" (17 Sep), "Kal" (19 Sep)

Filed 16 Sep 2026
Data requested Who registered the Web API key linked to this account, and from which IP / device / timestamp
Legal basis cited GDPR Art. 15 — right of access to personal data
The legal frame: Article 12(3) gives the controller one month from receipt (extendable with reasons). That period had not expired at publication, and this dossier does not assert a deadline breach. The objection is to the substance: the closing response links to a self-service page but does not show that the four named data categories were produced, and if the controller declines to act, Article 12(4) requires it to state the reasons and the complaint routes. Neither appears in the closing response.
Why this specific data matters
The Web API key event log is the record that shows whether a third party registered a key using a stolen session cookie — the mechanism described in the inventory-theft complaints preserved in this dossier's archive. Disclosing who registered an API key, from which IP, and at what timestamp, would:

- Allow the victim to compare the API creation IP against their own login history
- Reveal data-centre IPs linked to known phishing / gambling bot infrastructure
- Produce evidence usable in civil or criminal proceedings against the actor
- Show whether the account holder was notified when the key was created

What the record shows: Valve retains device-level and account-correlation records — its counsel's letter of 1 October 2025 describes them (see Appendix A, Evidence Memorandum — Source 1). In ticket HT-2YBP-F7JP-D4VB the same class of records was requested by the data subject and the ticket was closed with a referral to a self-service page that the data subject reported did not contain them. Whether that refusal is lawful is a question for the supervisory authority; the effect is that the person the data concerns does not get it.
The exchange — four messages, three days
Two Steam Support agents replied under first names shown on the ticket: "Logen" on 17 September and "Kal" on 19 September. Both referred the requester to the Account Data page. Nothing on the ticket shows whether the request reached Valve's Privacy Team or Data Protection Officer, and the dossier does not assert who the agents are, what their roles are, or how the ticket was routed.

16 SEP
Art. 15 request filed with four named data categories
17–18 SEP
Referral to Account Data; requester asks for DPO escalation
19 SEP
Ticket closed with the same referral; no data, no stated basis
What Article 15 GDPR explicitly entitles the subject to
Art.15(1)(a) Processing purposes — why Valve holds the data
Art.15(1)(b) Categories of data — what Valve holds
Art.15(1)(c) Recipients or categories of recipients — **who received the data (e.g., API key holder)**
Art.15(1)(d) Retention period or criteria for determining it

Art.15(3) A copy of the personal data undergoing processing — i.e., the API-key log itself ART.12(3) Response required within **one month** of receipt; an extension must be communicated within that month. The period had not expired at publication. **Art. 12(4):** if the controller does not act, it must state why and inform the subject of the complaint routes.
Regulatory complaint pathway — for any user
Any user who submitted an Article 15 GDPR request to Valve and received no compliant response (or a template refusal without data) may file a complaint with the supervisory authority in their EU/EEA member state. Valve's EU establishment is Valve GmbH in Hamburg, so the lead supervisory authority for cross-border complaints is the **Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI)**. (Valve's Article 27 representative is also located in Hamburg; a representative's address does not by itself determine the competent authority.) A complaint may also be filed with the authority of the complainant's own member state under Article 77.

HmbBfDI complaint form ↗ GDPR text (Art. 12, 15, 77) ↗ archived 2026-09-20 ↗ EDPB guidelines ↗
Ticket reference for any complaint: **HT-2YBP-F7JP-D4VB** — preserved in this dossier as a documented instance.

`One documented instance`

The records exist; the data subject did not receive them.

Valve's counsel described device-level correlation records in a letter of 1 October 2025. On 19 September 2026 an Article 15 request for the same class of records was closed with a referral to a self-service page the requester reported did not contain them, without a stated legal basis. Ticket HT-2YBP-F7JP-D4VB is one documented instance; whether it reflects a wider practice is a question for the supervisory authority, which can ask Valve for its handling records.

`GDPR Articles 12, 15, 77 / Supervisory authority`

A complaint under Articles 12 and 15 can be lodged directly with the relevant supervisory authority without cost (Article 77). The authority may impose corrective measures including orders to comply with the access request, and fines under Article 83(5)(b) for infringements of data-subject rights. Preserving the original ticket reference and any Valve response (or its absence) strengthens a complaint.

See the DSAR template →

`Part C — Legal frameworks · Section 19 · Contract law`

The Subscriber Agreement against the platform's own architecture

Context & source limits

The authors are not lawyers and none of this is legal advice. The SSA is quoted from the revision of 10 September 2026; a different revision may read differently, and clause numbering has changed across revisions — check the clause against the version that governed the conduct in question. The Articles 25 and 32 arguments state what the regulation requires, not that a supervisory authority has found a breach. The figures in Argument 1 carry the scope limits set out in Section 13.

Three of the SSA's central provisions sit awkwardly with how the platform is built: the commercial-use prohibition against a Market price ceiling that pushes high-value sales off-platform; the user-liability clause for API keys against a key endpoint that, before 2023, required no second factor; and the enforcement language against a public record that shows no per-operator enforcement. Whether these tensions affect enforceability is a question for a court; this section sets out the facts a court would have before it.

Argument 1 / Market Cap Architecture

The Market ceiling and the commercial-use prohibition

The Steam Community Market has a listing ceiling of about $1,800. Across five marketplaces in a dated snapshot (23 Sep 2026), 248 CS2 item categories are independently priced above that ceiling by two or more of them; such items **cannot be sold at those prices on Valve's own platform**. Owners who want those prices use third-party markets, which run on Steam accounts and the Steam API — use that the SSA classes as commercial unless expressly permitted.

Items exceed the Market ceiling → third-party markets fill the gap → those markets use Steam accounts and the Steam API → the SSA prohibits commercial use without permission → no register of permissions has been published. The Community Market's combined fee of about 15% applies only to sales completed inside the Market, not to these external trades.
Argument 2 / API Key Security Architecture

The API-key vulnerability as a platform design question rather than user negligence

Before 2023, Steam's API key creation endpoint accepted a POST with a stolen sessionid and generated a high-privilege credential **without e-mail confirmation, a second factor or device verification**. The API hijack complaints collected in this investigation follow one pattern: attacker script, stolen session cookie, silent key creation, trade interception (the request payload is shown in Section 8).

GDPR Article 25 (data protection by design) and Article 32 (security of processing) require technical measures appropriate to the risk. Issuing a credential capable of trade interception without a second factor or owner notification is a design question for the controller. Whether the SSA clause placing liability on the user can be relied on against that background is a question for a court and the supervisory authority.

Argument 3 / Real-Time Visibility

Valve receives the auth hostname on every login

The auth hostname arrives at Valve's OpenID endpoint in plaintext in `openid.return_to` and `openid.realm` (the request shape is shown in Section 3). Extracting it is a standard operation. As of 2026-09-22, in 26 pairs the main domain was on the Link Filter while the host carrying its Steam login was not. Valve has published no per-operator enforcement record, so whether any measure other than the Link Filter has been applied to these hosts cannot be established from public data.

Who bears the cost

The pattern in the archived complaints

In the reviewed complaints, Steam Support's response to an API-key hijack claim follows one form: decline restoration, cite the user's responsibility for the account and its API key, close the ticket. No aggregate figure for accounts affected or value lost is estimated in this dossier; no source for such a figure has been located.

The question is not whether individual users made mistakes. The question is who is responsible for an architecture that, until 2023, allowed a POST request with a stolen cookie to create a high-privilege trading credential with no notification and no second factor.

`The SSA as a document vs the SSA as a contract`

A court evaluating this record would not read the SSA in isolation.

It would read it alongside counsel's October 2025 letter describing device-level correlation, the auth-host registration dates, the batch registration timestamps, the API-key request payload, and the ten years between the July 2016 notices and the platforms still operating in September 2026. That is the record Valve would have to address.

`SSA against the record / key points`

- "No commercial use" — the Market ceiling pushes high-value sales to commercial third-party markets
- "Users liable for API keys" — no second factor on the key endpoint before 2023
- "We enforce against violators" — no per-operator enforcement record published since July 2016
- "You agreed to terms" — in the hijack pattern the acceptance is submitted by a script, not the account holder

`Conclusion · What the record establishes and what we ask`

The findings. The records we ask for.

Context & source limits

Each finding below is tied to a dated public record in the sections above. The requests are addressed to the authorities that can compel the one thing this investigation cannot reach: Valve's own enforcement, access and processing records.

Each request follows a dated finding. The authorities can seek records that this public-source investigation cannot compel.

What the public record establishes

1. 44 live platforms authenticate through a separate registrable domain — 27 with a published per-route evidence file, 17 from manual collection and listed apart. As of 2026-09-22, 26 pairs had the main domain blocked in the Steam Link Filter while the host carrying its login was not — csgogem.com blocked, `api.csgem.com` registered since March 2014. Steam receives that hostname in `openid.realm` and `openid.return_to` on every login. Section 3
2. On 13 July 2016 Valve publicly named the mechanism and prohibited it, and its counsel's notices of 20 July 2016 set a ten-day deadline. No per-operator enforcement record has been published in the ten years since that deadline. Section 11
3. The Steam Web API key endpoint issued a high-privilege, trade-capable credential from a session cookie alone, with no second factor before 2023. Section 5
4. A GDPR Article 15 request (ticket HT-2YBP-F7JP-D4VB) was closed after three days with a link to self-service and no data. Section 18

What we ask each authority

Washington State Gambling Commission
Reopen the 2016 file. Request an operator-by-operator account of which accounts, bots and return hosts were disabled after the ten-day notices, and which operators later regained access. Section 2

HmbBfDI (Hamburg; Valve GmbH)
Test whether the Article 15 response met the controller's duty, and require disclosure of the API-key registration and access records relevant to identifying the actor. Section 18

DSA digital-services coordinators
Put the auth-host routing on the record as notice, then assess whether Valve's response meets its obligations once knowledge is documented. Section 16

Any data subject
Use the Article 15 template to request the same records for your own account; a retained record can test who initiated a reset or created a key. Appendix G

The single request behind all four is the same: publish the enforcement, access and processing records that only Valve holds. A homepage warning, a ten-day letter and a self-service page are assertions of control. Whether control was exercised is a question the public record cannot answer and a regulator can.

Appendices — primary exhibits and working materials

Appendix A — Counsel correspondence

Evidence Memorandum — material provided by Source 1

Evidence base and source status for the counsel correspondence relied on in Sections 1, 18 and 19.

Evidence Base and Source Status — documents provided by Source 1
The user whose permanent ban triggered this audit is not the subject of it. Whether that ban was justified is not examined here, and this dossier neither defends nor disputes it. The account is not the point. What matters is the material: **Source 1** — the banned account holder, who received the correspondence below from Valve's counsel as the data subject of their own GDPR request — passed on that correspondence and the accompanying case files, together with the right to examine them publicly. The name is withheld; the documents are described by date, producer metadata and hash.

That correspondence was sent in response to a GDPR/DSAR request. In the course of it, Valve's counsel put a statement on the record, under signature, describing a capability that Steam Support had previously told users was not technically possible. The paragraph quoted below is that statement.

The authors' further analysis of the produced log extract is **withheld from this dossier** pending independent review. It is not relied on by any other part of this investigation.

`The admission on the record: persistent device-level telemetry`

In paragraph 1.9 of the letter attributed to Valve's counsel, Valve's attorneys state: *"Between 2019 and 2023, this account was used primarily from a device that was also used to log into dozens of stolen Steam accounts."*

The Fact: Valve's counsel here describes device-level correlation across accounts spanning four years. Steam Support has told theft victims that tracking stolen items or linking accounts to devices was not technically possible. Steam Guard device authorisation is publicly documented, so the existence of per-device records is not itself new; what is new is counsel's written confirmation that those records are retained and correlated across accounts over multi-year periods.

Why this matters: the correlation that can link one device to dozens of hijacked accounts over four years is the same class of record Support said it could not use for victims. Records of that class would be capable of identifying accounts and devices in a theft-and-resale chain. Which records exist, how long they are retained, and on what basis they are withheld from data subjects are the questions for the supervisory authority.
Source: letter of Valve's counsel dated 1 October 2025, paragraph 1.9, and its 830-page PDF appendix · received by Source 1 in response to a GDPR Art. 15 request · SHA-256 of the appendix recorded in disclosure-audit.json · the letter itself is not reproduced; account names and third-party data are omitted.

Status: open
Source materials are available through the evidence archive.

The redaction in the produced PDF is cosmetic: the covered text remains extractable

Valve's counsel answered a GDPR access request with an 830-page appendix in which the redactions are painted over the text rather than removing it. **902,270 characters sit under the black bars and come straight out with a text-extraction tool** — including the third-party identifiers the bars were there to withhold. Only aggregate counts are published here; no covered content is reproduced, and the appendix itself is not published.

1. What the geometry check found

The GDPR Art. 15 response dated **1 October 2025** was accompanied by an 830-page PDF appendix (Aspose.PDF for .NET producer metadata, created and modified on the same date). The authors ran a page-level geometry check: for each page, opaque near-black rectangles painted after the text layer were located and the extractable characters lying beneath them were counted.

Measured on the produced file

902,270
Characters still extractable from under the black bars
Counted, not estimated. This is a count of covered characters — not of victims, re-identifications or incidents.
830 / 830
Pages affected — every page
986
Rectangles over extractable text
1,329
Opaque black rectangles in total
The black bars are drawn over the text layer; they do not remove it. Text under the bars can be extracted with standard PDF tools. Only aggregate counts are published; no covered content is reproduced here.
Forensic Demonstration: Layer Separation
ASPOSE.PDF FOR .NET VECTOR OVERLAY MOCKUP (APPENDIX P. 412)
Report filed against account: [LOGIN: redacted_user_667]

Reason submitted by user: [TEXT: "User reports duplicate items in inventory and abusive trade conduct..."]

Foreground: <path fill="#000" /> Flaw: Underlying UTF-8 stream intact
Source: PDF appendix to the counsel letter of 1 October 2025 (830 pages, Aspose.PDF for .NET producer metadata) · measured by the authors, method and per-page counts in disclosure-audit.json · SHA-256 of the appendix recorded in the same file · the appendix itself is not published.

2. Why this matters for a data-subject response

Valve's counsel sent this file to a data subject in answer to a request for that person's own records. The bars on it are cosmetic: the text underneath was never removed, so the third-party identifiers the bars were applied to withhold went to the recipient along with the file. A redaction that lifts with a text-extraction tool withholds nothing, and it also leaves the recipient unable to establish what was disclosed and what was not.

Article 15(4) is the reason those bars exist at all: the right to obtain a copy must not adversely affect the rights and freedoms of others. That is the obligation this production did not meet. Whether it is characterised as a personal data breach under Art. 4(12) is for the supervisory authority to determine; the disclosure itself is measurable in the file, and reproducible by anyone holding the same bytes — the SHA-256 is published, the appendix is not.

What was under the bars was not account numbers. It was the body of user reports filed against the requester, with their authors attached: Steam logins that, because a login is rarely used only on Steam, identify the person behind them — **on the authors' count, over 60% of the users named in the document are fully identifiable** — together with the raw, unredacted text of what they wrote. That text includes death wishes and abuse directed at the requester's nationality. Some of the people so identified are minors. **The production handed a named list of reporters to the person they had reported**, which is the precise harm Art. 15(4) is written to prevent.

The sequence around the file matters as much as its contents. The request was met first with a demand for further proof of identity, on the ground that the requester's alias email address did not contain his name; the account was permanently banned during the delay that followed. The letter that finally delivered the data, more than six weeks past the Art. 12(3) month, threatened the recipient with criminal prosecution and withheld the remainder of his own data until he explained his account activity to counsel. The disclosure also settles two questions Valve has not answered in public: the records produced show account-linking reaching back to 2019, and internal telemetry of a depth Valve has never described.

Scope of this section: the observation here is limited to the mechanics of the redaction, measured on the file as produced. The authors' further analysis of the produced logs is withheld pending independent review and is not relied on elsewhere in this dossier.
Evidence: counsel letter of 1 October 2025 and its PDF appendix (SHA-256 recorded in the audit file); page-level PDF measurements and method ↗. The sequence of the request, the page-8 refusal and the characterisation of the exposed records are set out in full in PhishDestroy's account, "My Dog vs. Elite GDPR Lawyers", 17 August 2026 ↗ archived 2026-08-21 ↗. Account names and third-party data are omitted here; nothing covered by the bars is reproduced.

> **Page 8 of the covering letter refuses part of the request, and states the reason in writing:** "Eine genauere Auskunft ist aufgrund des Schutzes der personenbezogenen Daten anderer Nutzer der Steam-Plattform… nicht möglich." — a more detailed answer is not possible, because the personal data of other Steam users must be protected. The 830-page appendix was in the same package. What the bars covered was not account numbers: it was the reports filed against the requester, their authors

> named, with the raw unredacted messages attached. The account holder had asked Valve, through its counsel, for his own file; what he could extract from it was other people's. Nothing in this appendix turns on who drew the boxes. What it establishes is that the protection Valve invoked as its ground for withholding is the protection this same production failed, in the same envelope, on the same day.

Support and Legal Correspondence Exhibits

> Open the full visual catalogue and its source records online.

Appendix D — Source collection

Selected primary records

Six records from the archive — three GitHub issues in Valve's trackers and three Reddit accounts of disputed support outcomes. Each source stays attached to the claim, the saved text and the question it raises.

GH-01 / GITHUBOpen in saved build

Hardware keys, requested in 2016

ValveSoftware / steam-for-linux · #4521 · 2016-06-27

A user asked Valve to support U2F hardware keys as an alternative second factor. The saved issue carries both Feature Request and reviewed labels, with its state recorded as open.

> I request U2F usb dongle support in steam as an alternative.
>
> *Excerpt from the GitHub issue ↗*

Documented record
A dated request for an additional account safeguard, published in Valve's own issue tracker and labelled reviewed.

Accountability demand
Publish the product decision, the response date and the protection delivered after review.

Read saved record Open GitHub ↗
In the dossier: Account safeguards →Archive #484 · build 2026-09-17

GH-02 / GITHUBOpen in saved build

Crash reports without an effective opt-out

ValveSoftware / steam-for-linux · #6459 · 2019-08-18

The reporter describes a Steam client from 12 August 2019 on Ubuntu 16. They say disabling the crash-upload destination did not persist after a restart, and include the relevant configuration.

> If I disable the `ServerURL`, it gets overwritten after every reboot.
>
> *Excerpt from the GitHub issue ↗ archived 2026-04-19 ↗*

Documented record
A specific privacy complaint with a client date, operating system and configuration excerpt. The saved issue is open.

Accountability demand
Identify the investigation, the affected builds and the change that made the opt-out effective.

Read saved record Open GitHub ↗ archived 2026-04-19 ↗
In the dossier: Request the underlying records →Archive #467 · build 2026-09-17

GH-03 / GITHUBOpen in saved build

Auth-ticket abuse reported to Valve

ValveSoftware / Source-1-Games · #3857 · 2022-02-26

The author alleges that a server operation retained Steam authentication tickets after players disconnected and used misleading server listings. The post asks Valve to address the behavior.

> Making their servers look packed.
>
> *Excerpt from the GitHub issue ↗*

Documented record
A public abuse report lodged in Valve's tracker on 26 February 2022. Its saved state is open; the report includes links to screenshots.

Accountability demand
Produce the investigation result and the mitigation record for the reported authentication-ticket abuse.

Read saved record Open GitHub ↗
In the dossier: Dataset scope →Archive #768 · build 2026-09-17

RD-01 / REDDITAuthor's account

44 disputed Market purchases

r/DotA2 · author handle withheld · 2022-07-07

The author reports 44 unauthorized Market purchases on 6 July 2022 and roughly $500+ in losses. They say two-factor authentication was enabled and describe repeated template replies from support.

> 2nd ticket in and I have still yet to receive a non robotic copy paste template response from Steam.
>
> *Excerpt from the Reddit post ↗ archived 2025-03-20 ↗*

Documented record
A dated account of disputed purchases, with links to transaction screenshots and a support response. The amounts and events are the author's report.

Accountability demand
Reconcile the disputed purchases with transaction and session logs. Explain the evidence behind support's decision.

Read saved record Open Reddit ↗ archived 2025-03-20 ↗
In the dossier: Support and enforcement →Archive #4,533 · build 2026-09-17

RD-02 / REDDITAuthor's account

A permanent ban and closed appeals

r/ohnePixel · author handle withheld · 2024-12-09

The author disputes a permanent ban and says support cited suspected account transfer and community reports. They describe closed tickets and plans to request their personal data.

> I explained my situation and asked for more details, but they're sticking to their decision and closing my tickets.
>
> *Excerpt from the Reddit post ↗*

Documented record
A preserved appeal account, including the reasons the author says support supplied and links to four images. The post date comes from the selected support export.

Accountability demand
Identify the evidence supporting the permanent ban and the review available to challenge it. Closing an appeal does not explain the decision.

Read saved record Open Reddit ↗
In the dossier: Request the underlying records →Archive #4,766 · build 2026-09-17

RD-03 / REDDITAuthor's account

A recovery reset and a reported $10,000 loss

r/legaladvice · author handle withheld · 2025-05-09

The author alleges that support reset credentials and disabled account protections after someone else submitted a recovery ticket. They report a loss of about US$10,000 from an inactive account.

> Steam Support reset my password and turned off all my account security.
>
> *Excerpt from the Reddit post ↗*

Documented record
A preserved allegation about the recovery process overriding account safeguards. The saved post records what the author says support told them.

Accountability demand
Identify who authorised the reset, the ownership evidence they accepted and the access log. Account recovery is part of the security system Valve controls.

Read saved record Open Reddit ↗
In the dossier: Request the underlying records →Archive #4,592 · build 2026-09-17

Six selected records. GitHub states describe the saved build. Reddit posts preserve the authors' accounts.

Download the six records ↓

The searchable build contains **16,319 distinct records**: 393 Trustpilot, 5,635 Reddit, 2,395 GitHub, 276 web and 7,620 wiki records. Multiple records can concern the same event. The separate 40,448-row master export has a different scope.

Search the full archive ↗ · Build manifest ↗ · Dataset scope and counts →

Appendix E — Case study

ArchiSteamFarm and the automation clause

An open-source card-farming tool whose own FAQ states it runs on millions of accounts, set against the Subscriber Agreement clause (§ 4.C) that prohibits automation. The mechanics — what a farm has to buy from Valve before it can produce anything, why every way of cashing out a card breaches the licence, the enforcement record and who moderates the card economy — are set out in full in Exhibit V ↗.

The Steam Subscriber Agreement, § 4.C, states:

"You may not use any form of scripts, bots, macros, or other non-human-controlled systems ('Automation') to interact with Content and Services on Steam in any manner." — Steam Subscriber Agreement § 4.C (current) ↗ archived 2026-09-18 ↗

Valve enforces this clause. It is very good at it. The FAQ of **ArchiSteamFarm (ASF)** — an open-source tool its own documentation describes as running on **more than a few million Steam accounts** since a first release over 11 years ago — reproduces three Steam Support messages permanently banning users who ran bot networks. Valve found the networks, named them and killed them. The relevant question is therefore not whether Valve can detect automation at scale.

The project's official ArchiSteamFarm FAQ addresses the risk of a ban directly:

"This is extremely unlikely considering the fact that ASF is being used on more than a few million of Steam accounts, since its first release that happened over 11 years ago — but still a possibility, regardless of actual probability."

"Valve clearly acknowledges 'Steam idlers' existing, as stated here, so if you asked me, I'm pretty sure that if they weren't fine with them, they'd already do something instead of pointing out that they could cause problems VAC-wise. **The key word here is Steam idlers, for example ASF, and not game idlers.**"

— ArchiSteamFarm FAQ, JustArchiNET. Source: GitHub wiki ↗ · verified verbatim 2026-09-22

The same FAQ answers "Did anybody get banned for it?" with **Yes**, and reproduces what Steam Support wrote to three of them:

1,000+ bots · trade banned
"It looks like this account was used to manage a network of bot accounts. Botting is a violation of the Steam Subscriber Agreement."

170+ bots · permanently banned, 2017 Winter Sale
"this account was used to illegally collect collectible cards on Steam, as well as related and not only commercial activities. The account has been permanently blocked and Steam Support can not provide additional support on this issue."

120+ bots · permanently banned
"This and other accounts were used for flooding our network infrastructure, which is a violation of Steam online conduct."

— Steam Support messages reproduced in the ArchiSteamFarm FAQ, section "Did anybody get banned for it?". Source ↗ · verified verbatim 2026-09-22

Put the two records side by side. A private user with 1,000 farming bots is identified, told that "botting is a violation of the Steam Subscriber Agreement", and permanently removed. The commercial platforms in this dossier run automated Steam accounts as their core business, at far greater scale, and authenticate through Valve's own OpenID on every login — and no per-operator enforcement record has been published for any of them. **The clause works. The question is who it is pointed at.**

ASF is not accused of anything here, and its reading of Valve's position is its own — its author states plainly that "ASF is not authorized by Valve". The tool is used here as a measuring instrument: it shows that Valve detects bot networks, names them in writing and bans them permanently. Valve can close the question in one sentence by publishing which commercial automation it authorises, and the per-operator record of what it did about the rest.

`Where card farming touches Valve's revenue`

Farmed trading cards are sold on the Steam Community Market, which charges a combined fee of about 15% on each sale completed inside the Market; the account must have spent $5.00 USD on Steam before it can receive a card at all; and card drops require game ownership or in-game purchases. No aggregate revenue figure is estimated here — the operating scale is stated only as the ASF FAQ states it. The FAQ also records Valve distinguishing *"Steam idlers"* (card farming) from *"game idlers"*; see the ASF FAQ ↗. The mechanics are set out in full in Exhibit V — the scale and the commercial-use trap.

Subject ArchiSteamFarm — automated card farming
Stated scale Millions of accounts (per ASF FAQ — exact active count unverified)
Counted, not quoted 10,880,610 total API entries in ASF's own Steam group (5,360,499 non-limited, as Steam displays) — the FAQ's "millions" is not a story, it is a headcount. 88.97% carry no Steam ban of any kind. The full ban census ↗
Disclosures in the tool's own documentation

- ASF logs accounts in headlessly and idles games for card drops without launching the Steam client (per the project documentation).
- The FAQ reasons that Valve is aware of "Steam idlers" and that "if they weren't fine with them, they'd already do something".
- No targeted enforcement reported in over 11 years (per the FAQ); the resulting card sales inside the Community Market carry Steam's combined fee of about 15%.
- The FAQ states a recommended ceiling of ten accounts per operator and attributes it to Valve: "This recommendation is based on internal Valve guidelines, as well as our own suggestions." No such guideline is published by Valve.
- Technical ceiling, per the same FAQ: "you can run up to 100-200 bots with a single IP and a single ASF instance."
- Farmed playtime is recorded by Valve — "it's usually updated every 30 minutes or so" — and § 4.C lists "Faking gameplay statistics (e.g., inflated wins or losses, XP, playtime)" as a prohibited act.

Sources
Official JustArchi ASF FAQ wiki ↗ ArchiSteamFarm repository ↗ archived 2026-09-24 ↗
The automation clause is explicit; the ASF FAQ has stated for years that the tool runs on millions of accounts; no targeted enforcement against it has been reported. The gap between the rule and its application is the record; the reason for it is not established here.

`Full exhibit`

The card economy: the process, the scale, the licence and who moderates it ↗ What a farm has to buy from Valve before it can produce a single card; the two lines of § 4.C that name card

farming by its effects; why every way of cashing a card out breaches the licence Valve wrote while Valve charges a fee at the door; the enforcement record including the June 2025 VAC wave and chain-banning by shared phone number; and the Valve employee and community moderators found administering the card-trading and ban-list services around Steam.

The ban census

We didn't ask Valve how big the farm is. We counted it. ↗ 10,880,610 total accounts (limited and non-limited) read from ArchiSteamFarm's own Steam group, which the software auto-joins by default on first launch unless the user unchecks the group-join setting (capturing both commercial bot farms and regular players who left the default on). 88.97% carry no Steam ban of any kind; of the 11% that do, 99.8% are cosmetic community bans that never stop trading. Cross-checked against SteamRep, 67.77% of listed scammers walk free once anti-cheat bans are set aside. With registration-date, geography and survival breakdowns — the real scale, measured, not narrated.

Appendix F — Working ledger

Choose a rule. Inspect the matching records.

FSB Market is an anonymized label; the original criminal marketplace name is withheld here.

Context & source limits
Select a clause of the Subscriber Agreement or Online Conduct rules; the register lists the recorded platforms tagged under it, with their main domain, declared auth host and saved Link Filter result. The register describes the scope of this investigation's records, not a finding of breach against any platform.

Select a clause to see the tagged platforms, auth hosts and saved Link Filter results. Open each source to test the comparison.

Appendix G — From a template refusal to the underlying record

DSAR playbook: request the evidence

Use Article 15 GDPR to request personal data relating to API-key creation, account recovery and support access. A retained record can test who initiated an action and what the platform relied on.

1. 01

   ### Preserve your timeline.

   Save account notices, tickets, trade IDs and dates in UTC. Secure the account and review the recovery options applicable to the game and transaction.

   Steam Trade Protection information ↗

2. 02

Request your retained data.

Ask for timestamps, source IPs, key lifecycle events, security confirmations and account-related recovery actions. Include support-access events and recipients where those data concern you.

3. 03

Keep the delivery record.

Use Valve's privacy contact route. The usual response period is one month; a necessary extension of up to two further months must be explained within that first month.

Valve privacy contact route ↗ archived 2026-09-21 ↗

4. 04

Compare the response.

Reconcile logs with your timeline. Ask for reasons for omissions, then use the supervisory-authority complaint route if necessary. Preserve the response exactly as received.

Scope / Article 15

Access covers retained personal data, including data in logs. It does not guarantee every internal document, reconstructed records or unredacted data about others. Ask for an intelligible copy and the basis for any restriction.

EDPB access guidelines, §§ 2, 4–6 ↗ · GDPR Articles 12, 15, 77 ↗ archived 2026-09-20 ↗

Data subject access requestGDPR / Article 15

Account security & access records

Replace the bracketed fields before submitting.

```
To: Valve Privacy Team
Subject: Article 15 GDPR request — account security records

Account / SteamID: [YOUR ACCOUNT IDENTIFIER]
Relevant period (UTC): [START] to [END]
Related support tickets: [TICKET REFERENCES]

I request a copy of the personal data concerning me that you retain for this period, including:

1. API-key registration, confirmation, use and revocation events, with available timestamps, source
IP addresses, registered domains, device or user-agent information and non-secret key identifiers.

2. Recorded account-recovery actions, password/email/phone changes, Steam Guard removals or resets,
confirmation events and the account-related evidence relied on to authorize those actions.

3. Personal data in support-access and administrative-action logs concerning my account, including
available dates, purposes, actions and the support entity involved, subject to applicable rights of
others.

4. Account-related records used to determine any sanction, and available records of my complaints,
```

```
reviews and responses.

Please also provide the applicable processing purposes, categories, recipients, retention periods or criteria, and available information about sources where data were not obtained from me.

Where processing relies on my consent, please provide the retained record of the consent relied upon and the wording presented at that time.

Please provide an intelligible electronic copy with time zones and field definitions. Please do not include active credentials or secret tokens. If any requested data are not held, please say so. For any withheld data, please identify the scope and legal basis of the restriction and provide the remainder.

Please acknowledge receipt and respond within the applicable Article 12 period, explaining any necessary extension. I also ask you to preserve relevant existing records while this request is handled.

Name: [YOUR NAME]
Date: [DATE]
```

What a data-centre IP can establish

A discrepancy is evidence to investigate.

An API-key request originating from a data-centre network, as in the hosting-provider example raised in this investigation, can be relevant when compared with login records, confirmations and the user's timeline. An IP alone does not identify the actor or automatically defeat every defence. Evidence that a hostile actor supplied the recorded consent could challenge reliance on that consent; other legal bases and liability issues require separate analysis.

See the preserved ban-and-GDPR complaint →

Appendix H — Wayback Machine archive analysis · published support statistics

Support volume. Published response times.

Context & source limits
Valve publishes daily support statistics at `store.steampowered.com/stats/support`. Wayback Machine archives preserve historical snapshots of this page from 2018 to 2026. The volume-to-headcount ratio implied by these figures is inconsistent with per-ticket human review at the published response times.

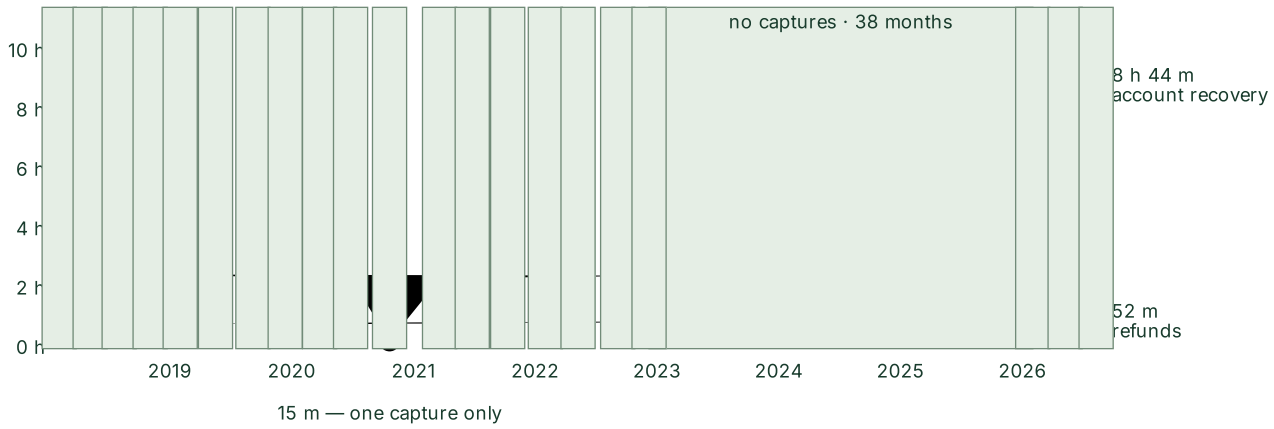
Compare Valve's archived support figures across the saved snapshots. The methodology explains what those figures can and cannot measure.

Volume against published response time (2018 → 2026)

Two queues at one support desk, read across 21 archived captures.

Valve publishes live support figures at `store.steampowered.com/stats/support`. Each point below is the lower bound Valve itself printed on that page on the day the Internet Archive captured it — not an estimate of ours. Both series are the same measure in the same unit, so they belong on one axis and can be read against each other directly.

Refund requests — money Valve is holding **Account security & recovery** — the account you have lost



49–55 min The refund lower bound in every capture from February 2018 to August 2026. Across eight and a half years it moves by under six minutes, while daily refund volume moves by a factor of nine.
2.4 h → 8.7 h The account-recovery lower bound sits near 2.4 hours in every capture through December 2022 but one. In the three 2026 captures Valve publishes 10.9 h, 5.8 h and 8.7 h.
×2.8 → ×13 How much slower recovery is than refunds, by Valve's own published figures. Steady for five years, then it widens — the queue that got slower is the one where the user, not Valve, is out of pocket.
Source: 21 Wayback Machine captures of store.steampowered.com/stats/support, 2018-02-03 to 2026-08-10; extraction in `VALVE_EVIDENCE_PACK/databases/steam_support_stats_history.json`. Read the limits with the figures: the chart plots the *lower* bound of the range Valve prints. The published upper bound is worse on both lines — refunds ranged 1.5 hours to 1.5 days, recovery 7.0 hours to 3.6 days. Two captures were archived in a localised edition of the same Valve page — 2018-11-03 in Czech, 2020-03-25 in French — and are marked (cs) and (fr) in the table; their figures appear here with the unit words translated and the numbers as published, and the verbatim source strings are kept in the extraction file. Every capture published a response time for both queues, and no point on either line is interpolated. The single 15-minute recovery figure of 2020-10-21 is flagged on the chart and left in: it appears in one capture only and no other capture is within an order of magnitude of it. No capture exists between 2022-12-08 and 2026-02-01; that 38-month hole in the record is shaded, and nothing is drawn across it. These figures describe published response times. They do not show what happens inside a ticket, and Valve has published no headcount against which to read them.

Open every capture as a table

Every archived capture, as published

Capture	Refunds / day	Refund response	Recovery / day	Recovery response
2018-02-03	98,788	50.12 minutes to 1.52 hours	25,662	2.51 hours to 1.80 days
2018-05-07	60,494	53.83 minutes to 1.47 days	24,226	2.45 hours to 2.22 days
2018-08-02	69,084	50.27 minutes to 1.59 hours	28,953	2.44 hours to 22.17 hours
2018-11-03 (cs)	63,410	49.28 minutes to 1.54 hours	33,910	2.42 hours to 1.31 days
2019-02-01	76,305	50.13 minutes to 1.52 hours	35,164	2.44 hours to 2.04 days
2019-05-18	78,951	51.03 minutes to 3.12 hours	27,514	2.46 hours to 20.39 hours
2019-09-07	78,941	50.65 minutes to 1.66 hours	28,812	2.42 hours to 13.59 hours
2019-12-13	69,589	50.77 minutes to 1.55 hours	25,322	2.45 hours to 1.13 days
2020-03-25 (fr)	139,278	49.45 minutes to 1.53 hours	32,302	2.48 hours to 3.62 days
2020-06-26	278,504	48.98 minutes to 2.29 hours	20,343	2.39 hours to 6.99 hours
2020-10-21	107,633	50.80 minutes to 1.54 hours	20,688	15.33 minutes to 8.62 hours
2021-03-20	158,956	50.80 minutes to 1.64 hours	25,760	2.34 hours to 11.62 hours
2021-06-26	547,907	51.93 minutes to 6.73 hours	29,728	2.40 hours to 15.63 hours
2021-10-10	170,103	51.88 minutes to 3.25 hours	23,989	2.39 hours to 13.05 hours
2022-01-31	354,386	53.65 minutes to 8.09 hours	24,391	2.42 hours to 15.29 hours
2022-05-09	172,555	51.83 minutes to 1.65 hours	23,289	2.41 hours to 16.90 hours
2022-09-05	153,453	53.67 minutes to 4.15 hours	23,594	2.45 hours to 1.22 days
2022-12-08	181,075	54.83 minutes to 6.67 hours	27,111	2.46 hours to 18.89 hours

Capture	Refunds / day	Refund response	Recovery / day	Recovery response
2026-02-01	317,762	50.30 minutes to 1.52 hours	47,197	10.91 hours to 21.30 hours
2026-05-09	246,776	50.12 minutes to 1.52 hours	35,264	5.81 hours to 15.60 hours
2026-08-10	373,244	52.05 minutes to 2.07 hours	45,319	8.73 hours to 16.52 hours

KEY OBSERVATION:
Across **21 Wayback captures** spanning 2018-02-03 to 2026-08-10, daily refund submissions ranged from **60,494** (May 2018) to **547,907** (June 2021) — a **9.1× spread**. The 2026 figure is 373,244 (+278% vs the February 2018 capture).
Over those same nine years the published lower bound for refund response time never left a **49–55 minute** band: a total movement of under six minutes while the workload behind it moved by a factor of nine.
If a person read each ticket for even 5 seconds, processing 373,244 tickets per day (current) would occupy **22 agents working 24/7** just to open and close them; at peak (547,907, June 2021) that rises to 32.
If the published response time reflected per-ticket handling time (~52 min/ticket), the implied concurrent staffing would be on the order of **13,500 agents** at current volume and ~20,000 at peak. No sourced figure for Valve's support headcount has been located; none is assumed here.
What follows: the volume-to-headcount ratio is inconsistent with per-ticket human review at the published response times. The figures are consistent with a largely automated first pass; what proportion receives human review is not published.
Why this matters for GDPR compliance
GDPR Article 22 prohibits solely automated individual decision-making that produces significant legal effects, without providing the right to human review on request. If Steam Support decisions (ticket closures, account actions, refusal of data requests) are made entirely by automated scripts, every such decision that "significantly affects" the user may violate Article 22.

Ticket **HT-2YBP-F7JP-D4VB** (Section 18) was closed after three days with a template referral and no engagement with the legal basis cited. Whether a person reviewed it cannot be determined from the ticket; that is a question the supervisory authority can put to Valve under Article 22 and Article 15(1)(h).

Source: Wayback Machine snapshots of store.steampowered.com/stats/support (2018-02-03, 2021-06-26, 2026-08-10) — data extracted into VALVE_EVIDENCE_PACK/databases/steam_support_stats_history.json (21 snapshots, 2018–2026). Note: the "~52 min" response time is the refund-category lower bound; account security response was 2.4–16.5 hrs across the same snapshots. 2021-06-26 is the all-time peak (547,907 refund requests), not a monotone midpoint — volume surged ~6× in 2020–2021 then partially fell before recovering to 373K in 2026.

Count the records. Check the scope.

Context & source limits
Count the records, then test the claims: every figure below is re-derivable from the published files.

Inspect the underlying datasets, reproduce the counts, and distinguish source rows from unique incidents.

The master CSV contains **40,448 rows**. Of these, **36,516** come from the Discord-AntiScam phishing feed. The remaining **3,932** rows span GitHub, reviews, search results, forum material and other sources, providing a comprehensive index of reported community topics and security reports.

Within that CSV, 1,690 rows are categorised under the "Unpatched Security Exploit" collection label, representing historical user issues and vulnerability disclosures. Tracing these reports involves reviewing each thread's specific build timeline and public patch history.

The 16,319-record searchable archive is a separate, curated build with its own manifest, designed for precise local exploration of specific user claims and incident reports.

> To build a reliable audit trail, every user-reported record must be verified against documented build timelines and historical patch logs.

The separate Part II collection records **231,829 unique listing IDs**, including 33,509 in the automated registration category and 198,320 flagged as unverified transfers. The input file's SHA-256 matches the preserved measurement. These counts describe listing attempts and observed transfers rather than finalized transaction values or verified theft totals, highlighting the need for primary platform records to measure the exact economic impact. Listing measurements and hashes ↗

Master CSV ↗ · Searchable archive manifest ↗ · Inspect source records ↗

The separate 17 October support collection adds **9,051 source rows**: 2,961 collector Tier A records and 6,090 Tier B reports. Its 5,727 research leads are excluded from that total. The collection includes repeated URLs, policy material and different outcomes; it is not a count of unique victims. Recomputed counts and source-image hashes ↗

Valve publishes no enforcement record. *We built one.*

Independent. Non-commercial. Built from public data only. Submitted to regulators.

88.97% automation fleet untouched — no ban of any kind
67.77% of 51,732 adjudicated scammers walk free
$26.8M+ floor on store spend by non-limited fleet
3.6% gambling domains blocked by Valve's Link Filter
8 years of security incidents documented

What this is. A forensic dossier into Valve Corporation's Steam platform — its enforcement record, its card-farming economy, its legal framework, and the authentication infrastructure that gambling operators use through Steam's own OpenID relay. Every figure is reproducible from two sources: Valve's own public API and the datasets published alongside this investigation.

Who it is for. Regulators with jurisdiction over Valve — the GDPR supervisory authority for the Netherlands, FinCEN, the SEC, the DSA Digital Services Coordinator, UOKiK, and any law enforcement agency examining Steam-linked financial flows. Also for journalists, researchers, and every user who received a permanent account ban, a refused refund, or a stolen inventory and was told there is no appeal.

The single demand. Valve holds this data at full fidelity — ban reasons attached, full ID space, real-time. It can run every query in this dossier in seconds and has chosen not to publish any of it. The question for any competent authority is simple: *why not?*

What the authors do not claim. No login to Steam was completed on any third-party platform during this work. A supplied OpenID URL establishes the request parameters, not a completed login. A separate registrable domain is not by itself proof of evasion. Registration dates are lower bounds on when a host could first have appeared in an OpenID request; they do not establish continuous use. The authors do not assert what Valve knew or intended: every statement about Valve is tied to a dated public document or a dated observation. Where a claim could not be put behind a source document, it has been removed.

Who we are
PhishDestroy — independent investigators. No affiliation with Valve Corporation or any platform named here. One Steam account was used solely to document the GDPR request in Section 18.

Legal disclaimer
Non-commercial, decentralized public-interest investigation. All data provided "as is" with zero warranties. This publication is not a judicial finding.

PUBLIC DOMAIN
Licensing
All rights surrendered to humanity. Reproduce, adapt, publish — attribution not required. OFAC-region access: prohibited. Full licence & disclaimer →

Read the claim. Check its source.

This reading edition was prepared on 18 October 2026 from the current English article. It retains the authored discussion and analytical tables in the source HTML. Navigation and interactive controls are removed. Interactive datasets remain linked rather than expanded into thousands of printed rows.

Selected source images remain linked to their publications or retained copies. The PDF does not independently authenticate the participants in a screenshot, verify every report in a collection, or determine the merits of a legal allegation.

Visual material linked separately

- visual catalogue: Support and Legal Correspondence Exhibits

Check this edition

The detached OpenPGP signature covers the exact bytes of the article JSON. That JSON includes the exported text, source identity and SHA-256 of this PDF. It is not a PDF document signature, and it does not certify the truth of underlying third-party material.

Article JSON · OpenPGP signature · JSON SHA-256
Published verification key · Verification instructions

```
Signing-key fingerprint
129FC7F39C40C69D2EF3C329BFCF9E8DD295EE01

Source HTML SHA-256
8f103fafacd97d0e3a3bae295ee280e63aa3f09b06288b07d33055f4a4bc249a
```

Reuse and attribution

Authored research is released under CC0 1.0 Universal. Third-party statements, screenshots and other source material retain their own rights and attribution. The original rights statement is a separate signed object.

```
Build 2026-10-18T11:58:30.589Z
Source: https://phishdestroy.io/steam_dossier/
```