

Section 19

# **The Subscriber Agreement against the platform's own architecture**

Investigated by: Agent Beatrix

The Subscriber Agreement against the platform's own architecture

## 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

[Download PDF](#)

[Download JSON](#)

[Download PGP signature](#)

PhishDestroy · file integrity signature for this fact

[Material record ↗](#)