ENGLISH · 18 OCTOBER 2026

Open Manifesto — Public Notice · The Steam Dossier

Open manifesto and public notice from the PhishDestroy team: forensic evidence of defective PDF redaction, Steam client network anomalies, and immutable IPFS data preservation. Investigation publishes 14 October 2026, unconditionally.

Prepared	18 October 2026
Attribution	PhishDestroy
Live article	phishdestroy.io/steam_dossier/open_manifesto
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 / 01 SECTIONS

Follow the record.

Article overview 3

A note on the countdown — why a timer is not a threat 6

Edition, sources & verification 8

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

Open Manifesto — Public Notice

Forensic evidence of forgery, backbone-level network anomalies, and immutable data preservation. Addressed to Valve Corporation, Taylor Wessing, regulators, and any observing intelligence agencies.

▲ OPEN MANIFESTO — PUBLIC NOTICE ▲
T-Minus · October 14, 2026
—
Telemetry Capture · Since Aug 31
—
10 regulatory bodies + originals **5** environments · running
Evidence: **IPFS** — immutable · daily commits
Reference: https://phishdestroy.io/steam_dossier

Subject: Open Manifesto — forensic evidence of forgery, network anomalies, and immutable data preservation. To: Valve Corporation, Taylor Wessing (the attorney who signed the disclosure [Exhibit A]), regulators, and any observing intelligence agencies.

▼ AnnouncementThe baseline — this is a record, not a negotiation

Let us establish the baseline. This is not a threat and not a negotiation. It is a record of facts already established and of actions already scheduled. We do not represent “Source 1” and we are not anyone’s proxy. We came for the phishing ecosystem — to prove that phishing operations reuse Valve’s styles, libraries, and OpenID infrastructure directly, and that Valve sees every one of them and does not ban them. In the process, we stumbled onto something bigger.

Your response determines exactly one thing: whether Valve appears in what follows as a participant or as a defendant.

What we seek is simple: an official answer and an admission of responsibility.

▼ §1The Taylor Wessing Disclosure — Publishes October 14, 2026

Valve will explain, publicly, what the attorney who signed the disclosure [Exhibit A] actually did in that letter and in that PDF. We understand they most likely did not fabricate the logs themselves — but they signed them and claimed them. So here is the question, and Valve will forward it to the bar regulator itself: why does a lawyer representing Valve produce documents like this — and are they even acting as a lawyer when they do? And how often has Valve, or its counsel, pulled this trick before?

This question goes to the regulator in any case. Your cooperation determines the framing, not the fact.

The investigation publishes on October 14, 2026 — unconditionally. Valve's official response, if provided, will be included verbatim and unabridged in all submissions. Silence will also be documented. The full investigation goes to 10 regulatory bodies, with the original letters and the original PDF sent by Taylor Wessing to Source 1 attached in unaltered form. Those originals show not merely an inability to operate a PDF, but — in our assessment, backed by a published mathematical audit — systematic evidence manipulation: organic Cyrillic harassment hidden, synthetic botnet reports left visible. The redactions are technically defective — documented and reproducible via our public forensic toolkit (gitlab.com/phishdestroy/taylor-wessing-data-breach-toolkit). The full methodology has been shared with regulators under confidential cover. The conclusion is mathematics, not opinion — and the mathematics says the responsibility cannot rest on the signatory alone.

▼ §2The Theft Ledger, the "Dupe" Fairy Tale, and the GDPR Charade

You will also resolve the account substitution fraud, the thefts, and the support negligence. How — internally or through regulators — is your choice. But understand what we are actually demanding:

▼ Stop lying about 2023

Trade substitution is happening right now, and we are watching it live. Valve patched the hole for exactly one game and declared the problem solved. Does Dota 2 no longer belong to Valve? Do Rust and TF2 players deserve less protection? A parallel investigation with full recordings and screenshots is already running — it will not go to regulators, but it will be published with facts, dates, and a complete description of the methodology that led us to them.

▼ The "million accounts" question

Valve wrote a figure to a prosecutor. Now Valve can answer publicly: how many accounts and in-game items has the company appropriated for itself? Not in prices — since Valve's official position is that these items are worthless — just a plain list of skins, and the reason Valve chose to keep them instead of returning them to the players they were stolen from. And while you're at it: you market the 7-day trade hold as an anti-scam measure. Explain how.

▼ The "dupe" fairy tale

We ask directly: what duplication are you telling your users about? Do you understand how absurd it is? A player owns a skin. The skin is stolen. For that player, the story is over. Whether Valve later bans the scammer or not changes nothing. Whether the skin ended up with the scammer or confiscated by Valve — for the victim, the outcome is identical.

▼ Your own support staff steals

We have documented two admitted facts of theft committed by Valve support employees. Meanwhile, players have no right of appeal against bans issued by those same support teams — possibly by Russian-speaking contractors. So: justify every ban. Prove to everyone that these bans are not the bias of the same support staff who stole skins. And since in the documented employee-theft case money was stolen — not skins — and the investigation traces it to specific wallets: state precisely which legal procedures Valve initiated against that employee in EU jurisdiction. Or none?

▼ Terminate the fictitious GDPR compliance

Your own lawyers' disclosure document proves the data was incomplete — by our verifiable estimate, roughly 1% of what Valve provably holds, by Valve's own admission about what it stores. Valve demonstrably does not understand what the law requires, and tries to buy its way out while its support openly lies and closes tickets. In Source 1's case the disclosure shows strong indicia of falsification — judging that is for regulators, not for us. But we state as fact: the data was not all there.

Our demand is primitive: stop lying. We will not stop, and we cannot be stopped — we are not one person, and our license is public. Either follow the law or openly abandon it. What you cannot keep doing is using the law as cover while hiding the profiles you ban for your own benefit. That is just ridiculous.

▼ §3The Steam Client Telemetry — Live since August 31 Live

Official announcement. For 32 days — since August 31 — the Steam client has been running inside our instrumented test environment, with user-level activity emulated around it.

The environment is strictly academic. It was built and is operated as a research setup, under certificates provided to us by a third-party research organization — not generated by us. This distinction matters, and here is why: Steam does not operate like an ordinary application. Valve functions at the level of backbone internet infrastructure, and at that level nothing behaves like "just packets" — routing, trust chains, and session handling all work differently. Self-signed certificates are simply not suitable for analysis at this level; the client would reject them or degrade. That is precisely why a legitimate, expensive, fully trusted certificate was required — and was provided to us for exactly this purpose. Your client accepted it. We see everything in plain text.

The setup, for your engineers:

- 5 independent environments. Two are physically equipped with GPUs — that matters.
- 1 system has games installed and played. 4 systems have zero games installed — a clean, logged-in, idling client.
- All five emulate an ordinary user: browsing, background work, consumer VPN usage.
- Every environment runs on our own hardware and network, using volunteer-provided accounts — one of them registered by a participant directly inside the research environment for this study. No third-party accounts, sessions or personal data are captured; captures are filtered to client-generated traffic before any archival to IPFS.

To be unambiguous: PhishDestroy is not a user, participant, or client of Valve or Steam. This is an observational study, and we do not conduct it in the first person — it is run together with a researcher at an academic institution. Tying this team to any individual account would be absurd.

We came to document phishing infrastructure. Instead we recorded backbone-level anomalies: on clean systems with no games and no downloads, the Steam client's packet sizes and structure shift in response to user activity outside of Steam. We do not yet know how to

classify these packets — but we know the people who do. And based on what is already being written to the network, we may end up with very serious questions — not only to Valve, but to NVIDIA — backed by facts, not speculation.

We understand the risk of what we are doing. We state plainly: we cannot judge whether what we observe is malicious by design or negligent by architecture. That judgment is not ours to make. But we are in possession of established facts that force the question regardless: Valve's documented cooperation with the Russian Federation and its regulators, and the fact that the support employees who stole users' skins were citizens of the Russian Federation. Combine this with what is already known: support employees hold extensive access to user data, no one controls that access, and no one controls whom they pass this data to. We are therefore compelled to raise this question publicly, independent of any other issue in this dossier.

It is precisely because of the risk attached to this data that we publish it to IPFS daily, as it is captured. No one can delete it. Not them — and not us.

We would have asked Edward Snowden to help interpret anomalies of this class. But we are not you — we do not maintain contacts with a terrorist state. Western regulators and independent researchers will do the classification instead.

Part 3 publishes when the dataset is complete. Right now we have more questions than answers — and every day of silence adds another immutable day of data.

▼ **§4Notice to Intelligence Agencies & Regulators: The Immutability Protocol**
To anyone considering pressure, seizure, or a takedown — read carefully.

All intercepted telemetry is written to IPFS in real time, cryptographically signed, and anchored to a multisig wallet that does not exist. The keys required to alter or delete this data were never generated or are provably destroyed. We cannot delete this data even if we want to. No court order, no coercion, no force applied to us can remove a single hash.

Every record carries its original embedded timestamps. Examine them, and the dates speak for themselves — the timeline is self-evident and self-authenticating.

An IPFS hash is immortal. The evidence chain no longer depends on our existence, our freedom, or our cooperation. It grows every day you remain silent.

The math is public. The originals are preserved. The capture is running. Answer.

— The PhishDestroy Team

A note on the countdown — why a timer is not a threat

The countdown above is not coercion and not blackmail. It is the opposite. Law in every relevant jurisdiction distinguishes between malicious action and good-faith resolution: a party that acts without first attempting resolution acts in bad faith. We are required to attempt

resolution before escalating — and this page is that attempt, made publicly, with a stated date. The timer exists so that no one can later claim there was no notice, no opportunity, and no good-faith window. It is the legal record of ours.

Valve understands this mechanism — and has already demonstrated it. When our previous notice period expired, infrastructure linked to Valve accessed Source 1's website on the very day of expiry and reviewed precisely the material that had been disclosed. They watched the deadline. They know what it means. Access logs are preserved.

A deadline you can see is not a threat. A deadline is what distinguishes a lawful demand from an ambush.

Public sources. Documented conduct. · PhishDestroy

EDITION NOTES / TRACEABLE FILES

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.

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
02cc1052c80b7f5d0e75b60e6d03cab7daa05f6184acaf57654253776240 0f63
```

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/open_manifesto
```