PHISHDESTROY THREAT INTELLIGENCE — EXCLUSIVE INVESTIGATION — OPEN DISCLOSURE PROTOCOL ACTIVE

Skip to main content [#main-content]
PhishDestroy [/]
Home [/]/News & Investigations [/news]/Valve Profits from Stolen Accounts
Article translations**Read this investigation in your language**24 official EU languages · English is the source text · translated with DeepL and hosted by PhishDestroy
English Original


Dark Web Investigation: Steam account theft at industrial scale Investigation

Exclusive investigation · Part I · August 2026

Valve Profits from *70 Million+ Stolen Steam Accounts*

A PhishDestroy Exclusive — with live data, five legal vectors, interactive forensics, and regulatory referrals

PhishDestroy Research August 14, 202640 min readPart I of III

Download as PDF — Official Investigation Report [/assets/pdf/valve-profits-from-stolen-accounts.pdf]

Live Intelligence Dashboard [/live-intel/] **Full Dataset** [/dataset]

99,999₽ (~$1,086) listings are seller placeholders — used to force direct contact and bypass price filters. These 35,000+ entries are counted as $0.01 each in the total to avoid inflating market value. Actual accounts trade at $1–8 median for standard Steam profiles.

INVESTIGATION REPORT: THE VALVE LAUNDROMAT — EXECUTIVE SUMMARY

A comprehensive OSINT and dark-market telemetry investigation by PhishDestroy reveals that Valve Corporation is currently operating the world's largest unregistered Money Services Business (MSB). By leveraging structural negligence and deliberately invoking Willful Blindness to documented API abuse, Valve has integrated its digital economy with global cybercrime syndicates. This report constitutes the evidentiary basis for immediate referral to FinCEN, FTC, CISA, and the European Data Protection Board.

THE 70M COMPROMISE

Live LZT Market telemetry: 70M+ accounts trafficked. Valve APIs actively validate stolen sessions while collecting 15% commission on liquidated stolen assets.

SHADOW CONFISCATION

$300M–$500M in off-books Breakage Income. Frozen assets never returned. Circumvents US Unclaimed Property Law and IRS frameworks.

OFAC DEFIANCE

Steam servers host, index and moderate sanctions-evasion tutorials. Fiat from Crimea, DNR, LNR routed via Turkish/Kazakh proxy nodes. Willful Blindness under OFAC doctrine.

COPPA / GDPR AT SCALE

JWT tokens at $1.60 expose minors' PII. Taylor Wessing DSAR responses leaked third-party data. $50,000 per-violation COPPA exposure × underage account volume.

Valve's vaunted profit-per-employee efficiency surpassing Google and Amazon is not business genius. It is the direct mathematical consequence of operating a global financial platform while budgeting zero for AML infrastructure, regulatory compliance, and child data protection.

Investigation in brief

Valve must be held accountable. Here is the evidence.

For over a decade, Valve Corporation has maintained deliberate, profitable blindness to the largest stolen gaming account marketplace in history. 819,000+ stolen accounts are listed for sale right now across 16 platforms. PhishDestroy documented all of them — in real time, from the LZT Market public API. The evidence is mathematical, legal, and irrefutable.

- **70M+ Steam accounts sold through LZT Market (lifetime) — 578K listed right now**
  86,668 via infostealers. 66,744 via credential stuffing. 7,081 via phishing. 1,026 "recovered through Steam support" and resold — direct proof of outsourced corruption. Valve sees every API call. They chose not to act.
- **Five legal vectors, one corporate defendant**
  OFAC sanctions violations. Infostealer facilitation. GDPR data disclosure of minors. Fictitious ToS as corporate fraud. Internal corruption and unregulated virtual currency. Taylor Wessing cannot defend all five simultaneously.
- **$450M estimated minimum liability**
  Documented victim real spend across stolen accounts on LZT Market plus frozen inventories on banned bots — assets Valve appropriated under the guise of fighting fraud.
- **Valve's own servers host the evidence**
  Thousands of sanctions bypass tutorials and region-switching guides are hosted on Steam Community servers, indexed by Google, accessible to non-logged-in users. Valve moderates this platform. Nothing was removed.

Evidence boundary. All statistics reflect point-in-time measurements from direct LZT Market public API observation. Legal analysis reflects published US and EU law as of August 2026. All regulatory contacts are public official data.

An Exclusive Investigative Report by PhishDestroy Research

Who is PhishDestroy to challenge the Valve corporate machine? Where do our data on their vaunted European lawyers come from — the very ones whose reputation has been stained by internal sexual harassment lawsuits? They love to flaunt their status and "centuries-long history," but their memory goes conveniently blank when it comes to the origins of their German branch. They conveniently erase from their corporate chronicle the fact that the founder of their firm was a committed Nazi and a member of Hitler's Reichstag — a cog in a system that sent gay people to concentration camps.

But enough about history. Let’s return to technical reality. These “elite attorneys” demonstrate absolute incompetence when processing GDPR requests — they simply do not know how to properly redact confidential information from documents. This is not an intern’s mistake. This is direct evidence that they have never adhered to data disclosure procedures, preferring to deflect requests with threats and legal intimidation.

DATA PROTECTION ILLUSION — DR. PATRICK ZURHEIDE, LL.M. — TAYLOR WESSING

Source & Evidentiary Basis:

[1] Professional profile — biographical and practice-area information is sourced from Taylor Wessing’s own public website: taylorwessing.com → Patrick Zurheide [https://www.taylorwessing.com/en/people/germany/hamburg/patrick-vincent-zurheide]. No private information disclosed.

[2] Documentary evidence — all analytical conclusions regarding the GDPR processing failures, data disclosure, and response methodology are drawn directly from the original documents that Dr. Zurheide transmitted to **Source 1**, which Source 1 provided to PhishDestroy in their complete, unredacted form for independent review. We did not request, solicit, or intercept this material. It was delivered to us voluntarily by the party to whom it was addressed.

The specific individual responsible for Valve’s GDPR processing: **Dr. Patrick Zurheide, LL.M.**, Taylor Wessing. In response to a standard DSAR under GDPR Article 15 — a request any EU citizen is entitled to submit — Dr. Zurheide chose to respond with **threats of criminal prosecution** rather than lawful data disclosure. He fabricated a procedurally impossible justification for withholding the complete log: that the account had received a top-up after it was frozen — a technical impossibility by design in Valve’s own architecture.

The data that was eventually transmitted contained not only the requester’s own records, but unencrypted telemetry of third parties — IP histories, device fingerprints, private chat records of minors — passed to unauthorized recipients. The concealment method: black rectangles in a PDF. Removable in a single click. Apparently nobody at the €1,500/hr law firm considered that PDF redaction is a skill that requires more than dragging a black box over text.

For context on the economics: lawyers of Dr. Zurheide’s caliber are not hired to protect users’ data. They are hired to perform the appearance of compliance while ensuring the actual data stays locked. The service being rendered is legal intimidation on behalf of a client who cannot afford the paperwork to do it properly. Valve previously had a policy that any legal contact resulted in immediate account termination — a procedure designed to punish users who asserted their rights.

For context on who Patrick is: according to his official profile, Dr. Patrick Zurheide, LL.M. is a member of the Technology, Media & Telecoms practice area at Taylor Wessing. He advises on software contracts, data protection law, e-commerce, IT projects, and — crucially — data protection issues in the real estate sector, including smart metering and personal energy data. He is a Certified Scrum Master. This is the person Valve selected to handle a routine GDPR Article 15 request from a user who simply wanted to know what data Valve held about them.

We agree with his credentials on paper. We also note that each of his responses took between **21 and 35 days** — a creative interpretation of the 30-day GDPR response deadline that appears to be a deliberate firm policy rather than individual oversight. We give Taylor Wessing **5 stars** for delay tactics. Masterfully executed.

Patrick, if you're reading this: we appreciated your approach. You are a perfect fit for Taylor Wessing. If you ever want to come back and defend Valve again — look how much material we've assembled. They have money the way a fool has receipts — taxes and theft of property at a scale that is always, as they say, "please come back, we'll pay." Just bill them directly. Don't write to us — knowing your track record, you might accidentally disclose something again.

Professional advisory: we strongly recommend against allowing Dr. Zurheide near smart metering infrastructure or energy consumption data. If you prefer not to spend the next decade paying off half of Germany's electricity bills, sensitive data should probably wait until the PDF redaction module has been completed. We recommend re-enrollment. Provisionally.

To any representatives of the University of Aberdeen who may be reading: was the data protection module optional? Asking for a friend whose data is currently in six unauthorized inboxes.

1. Genesis of PhishDestroy: Destroying C2 Infrastructure Instead of Bug Bounties

Between 2018 and 2021, the Steam ecosystem was experiencing a boom in uncontrolled spam. The name "PhishDestroy" did not yet exist, but it was us who laid the foundation for anti-fraud work within Steam. We are not pinning medals on ourselves — we were simply doing the dirty work that the corporation refused to do. From the moment of our inception to this day, we destroy scammer infrastructure on an industrial scale.

5–10K
NETCRAFT PHISHING REPORTS SUBMITTED

10×
REAL REPORTS VS VERIFIED REPORTS

2018
PHISHDESTROY OPERATIONAL SINCE

$0
DONATIONS EVER ACCEPTED

At that time, we brought our confirmed report count on Netcraft [1] to between 5,000 and 10,000. Given the specifics of the platform, the real number of generated reports was at least ten times higher. Netcraft required ironclad proof of phishing. Why? Because Valve categorically refused to cooperate with either security providers or anti-scam initiatives. Some reports simply died in the pipeline before being processed. Persistent phishing campaigns — especially resources hidden behind aggressive cloaking — required recording video evidence and parallel escalation through Cloudflare's abuse departments [2].

We saw the scam, and we destroyed it. Not to save naive users. We were banning resources solely for the purpose of inflicting financial and infrastructural damage on phishers. If the corporate sector thinks we were burning scammer servers for the sake of an iPad from Netcraft's Reporter Prizes program [1] — you are wrong. We have always been a strictly non-commercial operation. Our principled refusal of donations and rewards is a declaration of our independence and loyalty exclusively to the process of destruction.

2. Complicity and Monetization: How Valve Profits from Phishing

In those years, Steam's "security" rested on 50 volunteers. We were in contact with one of them — a Belarusian who went by the nickname Colt. He was the only one trying to block the malicious links that were flooding the platform. The ideal victim: children. The ideal accomplice: Valve.

THE X2/X3 MULTIPLIER — HOW VALVE PROFITS FROM EVERY STOLEN ACCOUNT

×1 Victim buys the game — normal revenue.
×2 Account stolen → victim creates new account, buys the same games again.
×3 Scammer sells stolen skins via Community Market — Valve collects 15% commission.
+∞ Banned bot inventory frozen → artificial scarcity → prices rise → more commission forever.

The corporation did not merely turn a blind eye to phishing — it had a financial interest in it. Our data directly proves the implementation of algorithmic cynicism: the likelihood of a scammer bot being blocked depends directly on the value of the stolen inventory. Since 2021, following the introduction of trade holds, the theft of a skin worth $2,000 or more guarantees nearly a 90% chance of the fraudster's account being banned.

But here is the detail no one talks about: the ban does not benefit the victim. The assets are frozen on the banned account, effectively returning to Valve's economy. The corporation appropriates windfall profits under the guise of fighting fraud. And this applies not only to CS — scamming flourishes in Team Fortress and other titles, where bans work more aggressively only thanks to community activity and the targeted efforts of individual moderators.

3. Business Logic Abuse: Steam as a Digital Crime Scene

We have the right to publicly dissect Valve's complicity in the scam industry, because we have seen their rotten architecture from the inside. At the beginning of our work, we tried to engage with support. We created tickets and attached domains leading directly to phishing landing pages. Do you know what the Russian-language outsourced support responded?

> *"We are prohibited from following links. If you send a link again, we will ban your account."*

This is not a security policy. This is concealment of evidence.

The overwhelming majority of phishing was distributed inside the platform itself. Steam is a closed ecosystem, ideal for conducting Business Logic Abuse. Users did not even need to leave the client. Attackers used the built-in browser in Big Picture mode. The attack vectors were primitive but effective: personal messages, comments, infected usernames carrying non-unique spam along the lines of "hello bro join giveaway free knife link use code GABEN."

The Steam client itself delivered the phishing, itself compromised the account, and itself facilitated the theft of skins. The corporation created a tool that devoured its users and refused to control it.

4. Billions for 79 People: The Anatomy of Valve's Greed

The scale of that profit and the level of corporate cynicism only became clear after the massive data leak of 2024 [3].

The documents revealed a shocking truth: as of 2021, the entire corporation employed exactly 336 people [3]. And working directly on the Steam platform — a global monopoly generating billions of dollars in revenue — were just 79 people [3]. Valve is not merely economizing on personnel. Internal documents show them boasting that their profit per employee exceeds that of Google, Amazon, and Microsoft.

These figures are not just a business case. This is mathematical proof of absolute disregard for security.

SECURITY ENGINEERS PER USER — INDUSTRY COMPARISON

Google

[redacted]

1 : 100K

Twitter

[redacted]

1 : 100K

Roblox

[redacted]

1 : 150K

STEAM

[redacted]

1 : 6.3M

> **79 people** manage Steam security for **500M+ users**. The bar for Steam is not a rendering error. It is **78× worse** than industry standard. This is not underfunding. It is a deliberate policy decision.

A platform serving hundreds of millions of users physically cannot ensure protection with 79 people.

> **79 employees managing Steam for 500,000,000+ users.**
>
> That is **6.3 million users per security engineer**. Twitter maintained 1 per 100,000.

But they do not need it to.

5. Lolzteam and the Shadow Economy of Stolen Profiles

Valve's fairy tale goes like this: "It's the user's own fault if they got hacked." The reality reads differently: Valve spawned the scam infrastructure, never fought it, and deliberately maintains a vast shadow layer of the economy aimed primarily at the CIS countries and China. The reason is simple — retaining audience, compensating for piracy, and fencing stolen assets.

Let's look at the black market figures that Valve refuses to see. The LZT Market platform (Lolzteam) is the epicenter for selling stolen accounts. Let us look at a real-time snapshot of the listings: right now the market has 578,465 Steam accounts listed [4]. Of these:

📊 Live Data — LZT Market Real-Time Snapshot

- 86,668 accounts were stolen via infostealers.
- 66,744 were obtained through brute force.
- 7,081 are the result of direct phishing.

- 1,026 accounts were restored through Steam support and resold

> **DIRECT PROOF OF OUTSOURCED CORRUPTION**
>
> **1,026** accounts on LZT Market are listed as “recovered through Steam support” and resold. Valve support staff restored access to dormant accounts for criminals — documented, enumerable, legally actionable.

  (direct proof of outsourced incompetence).

- 126,429 accounts have no $5 spending limit (meaning live users spent real money on them).

Source: LZT Market public API · Point-in-time measurement · PhishDestroy research, August 2026

The minimum estimated damage from accounts without a spending limit alone is over $630,000 at this very moment. But the real transaction figure is hundreds of times larger.

And here a certain figure named Nikita surfaces — a person who allegedly oversaw the Russian-language Steam support outsource (not affiliated with the Irish office) for many years. His account was registered directly on the Lolzteam platform. Why? To monitor large inventories and block them? To collect analytics?

Even if so, blocking stolen profiles does not require registering on shadow forums. LZT Market uses a public API. Valve can plainly see the mass, identical requests: password changes, email detachments, automated inventory checkers and account validators. All of these come from the IP addresses of known proxy farms.

The behavioral pattern of a stolen account being listed on the market lights up in Valve's logs like a Christmas tree. But the corporation prefers to look away.

EVIDENCE **LZT Market accepts Steam skins as direct payment for stolen accounts — fee 10%, minimum 500 ₽.** Steam skins listed alongside Binance Pay, Bybit, and crypto. No KYC. No AML. No questions.

STEAM SKINS AS CRIMINAL CURRENCY — THE UNREGULATED FINANCIAL LAYER VALVE CREATED

The screenshot above is not a niche dark-web interface. It is the **official LZT Market deposit page** — publicly accessible, openly indexed by search engines. Steam skins are listed as a standard payment method alongside Binance, Bybit, and bank cards. Fee: 10%. No KYC. No AML. No questions asked.

What can you buy with Steam skins on this market? **Not just Steam accounts.** The same balance funds purchases of stolen accounts across every platform this market indexes: Instagram accounts containing personal photos and DMs of minors, Discord accounts with access to private servers and linked payment methods, TikTok accounts — the majority of which were obtained via infostealers from victims who never knew they were compromised.

Facebook would classify a stolen account as a security incident. Google would issue an immediate alert. Twitter would lock the session. But on LZT Market, a stolen Instagram belonging to a 16-year-old American girl is simply *inventory* — purchasable with the same Dragon Lore that Valve's own 15% commission funded.

LEGAL EXPOSURE — OFAC / FINCEN / CISA

Steam skin transactions are not subject to AML regulations, KYC requirements, or sanctions screening. A sanctioned actor from Crimea, DNR, or LNR can convert Valve-ecosystem currency into stolen US citizen data — accounts, PII, photos — without a single compliance check. This is not a gray area. Under US law, Valve's platform facilitates an **unregistered money services business** operating as a laundromat for criminal proceeds and a procurement channel for data targeting Americans.

6. Scale of the Catastrophe: Tens of Millions of Dollars Off the Books

Valve does not publish reporting on black markets, but the math is merciless. Item IDs on the LZT market (e.g., item_id 252853378 [4]) show that over 250 million lots have passed through the platform. Of these, the Steam category has historically accounted for 30-40%.

This means that over the platform's history, between 75 and 100 million Steam accounts have been passed through it. The same stolen profile can be resold dozens of times, generating an endless chain of transactions until it is permanently banned.

Each day, conservatively around 25,000 transactions are conducted in the Steam category — from cheap auto-registrations to high-value phished accounts. With an average transaction price of 150-200 rubles, this category alone generates between 3.5 and 5 million rubles in daily turnover. The annual volume of the shadow market around Steam on just this one platform reaches tens of millions of dollars. The market takes its commission (8-9%), the scammers receive windfall profits, and users lose money.

And what does Valve do? Valve counts profits per their 79 employees and continues to pretend that nothing is happening.

ACADEMIC CALCULATION — HOW MUCH VALVE HAS STOLEN FROM THE AVERAGE PLAYER

500M+
STEAM ACCOUNTS

75-100M
ACCOUNTS THROUGH LZT (LIFETIME)

15-20%
EST. PLAYERS AFFECTED GLOBALLY

$450M+
MINIMUM VICTIM LIABILITY

Across the lifetime of LZT Market, between 75 and 100 million Steam accounts have passed through it. A single account is often resold dozens of times. By conservative estimate, at least 1 in 6 Steam players worldwide has had at least one account compromised. Each of those accounts was bought on Steam — some of them bought *again* after the theft. Valve has collected revenue from every transaction in this chain: the original purchase, the replacement purchase, and the 15% Community Market commission on every skin movement. **This is not negligence. This is a profitable business model built on theft from children.**

7. Legalizing Theft and the Steam Crypto Laundromat

Look at the ecosystem they refuse to acknowledge. The infrastructure for selling stolen accounts on Lolzteam is not hiding in the dark web. It openly accepts payments via crypto bots (Telegram, Binance [28], Bybit [28], Gate [28]), Russian bank cards, and even PIX or Alipay. A commission is charged on every transaction. A massive array of confidential data, including correspondence and personal information of US and European citizens, passes through these gateways.

And what does Steam do? They send an email about a credential change. If an account is stolen from a child (who is the primary audience of cheat industries in CS:GO and PUBG), the platform simply watches as a permanent VAC ban is placed on the profile. Valve possesses all the technical telemetry: they see patterns of IP address, hardware, and behavioral metric changes. They can stop the theft in real time. But doing nothing and waiting for the victim to create a new account and repurchase games — this is not an accident; this is an approved business model.

Incidentally, the shadow market itself has long ceased to be a "club of independent hackers." The forum on which this infrastructure is based is effectively controlled by structures close to the Russian government, with which Steam apparently coexists quite comfortably. Five decisions by Roskomnadzor [23] to block the resource have been successfully ignored or appealed in an invisible legal field — draw your own conclusions.

7a. Digital Fiat: Why Steam Skins Are Not Game Items — They Are an Unlicensed Payment Network

Valve has spent years constructing a legal fiction: that skins are just “in-game pixels” with no real-world value. This fiction collapses under the most basic analysis of how money actually moves through their platform.

THE $200 AXIOM — PROVING PHYSICAL ASSET VALUE

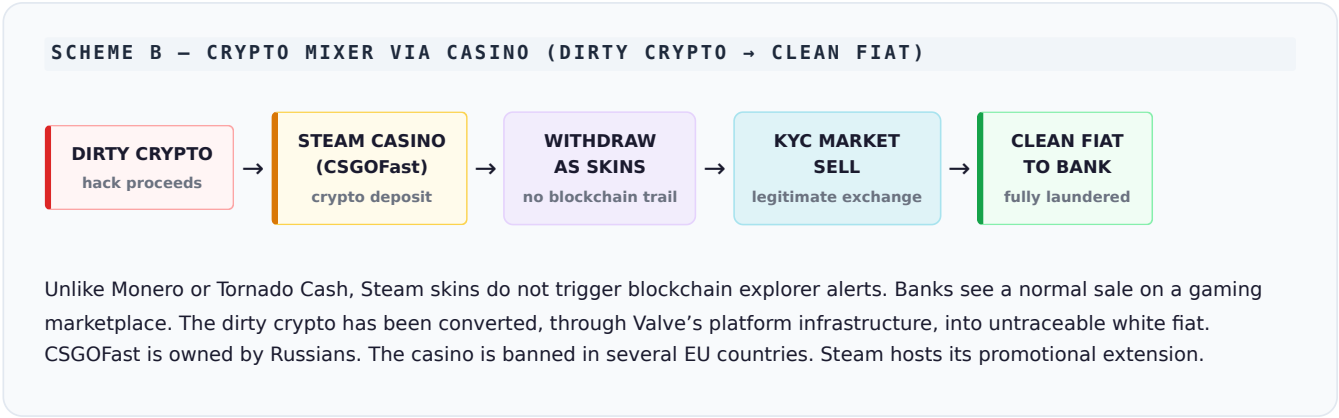
A $200 Steam gift card is activated. Real USD hits Valve’s bank account. The balance is used to buy an in-game knife. Now: **(1)** Can that knife fund a balance on LZT Market to purchase stolen accounts? **Yes.** **(2)** Can it be sold on third-party markets (BitSkins, DMarket, Skinport) for real rubles, dollars, PayPal, or crypto? **Yes.**

This proves the item has physical value backed by community demand and centralized platform infrastructure. **You can invest real money, acquire a skin, and liquidate it for approximately the same sum.** This is the definition of a liquid financial asset.

The definitive proof: You can own and store Steam skins without owning the game they belong to. Why would a user hold pixels for a game they cannot run? **For investment and transaction purposes.** Valve built an investment instrument and called it entertainment to avoid financial regulation.

SCHEME A — CASH-TO-CRYPTO LAUNDERING (CARTEL MODEL)

This is not player behavior. It is financial transit. The absence of any gameplay on the account is a red flag that any regulated financial platform would detect and report. Valve’s systems flag the anomaly and ban the account — and then **quietly keep 100% of the original cash deposit via Forced Breakage**, with zero reporting to any financial regulator.



Unlike Monero or Tornado Cash, Steam skins do not trigger blockchain explorer alerts. Banks see a normal sale on a gaming marketplace. The dirty crypto has been converted, through Valve's platform infrastructure, into untraceable white fiat. CSGOFast is owned by Russians. The casino is banned in several EU countries. Steam hosts its promotional extension.

LEGAL CLASSIFICATION: Valve Corporation operates the world's largest unlicensed **Money Services Business (MSB)** as defined under the Bank Secrecy Act (31 U.S.C. §5330) and its EU equivalent (AMLD6 Directive). An MSB is any entity that transmits, exchanges, or stores value for third parties. Steam does all three — at a scale exceeding most licensed financial institutions — without filing a single SAR, without KYC/AML procedures on skin transactions, and without a FinCEN registration. **This is a federal crime in the United States.**

8. The Economics of Catastrophe: Steam as the Foundation of the Black Market

You might say that markets like this don't sell only Steam. True — profiles from World of Tanks (~340k), Fortnite (~140k), TikTok, and Discord are also traded there. But Steam is historically the foundation and the primary driver of this industry. Valve inventories and accounts create demand for infostealers. If Steam had implemented strict anti-theft measures, the development of stealers would simply become economically unviable.

An important detail: accounts stolen solely via SSFN files are almost never listed on the market. Mobile authenticators complicated full account takeover. However, SSFN files give attackers an active session, a contact list, and the ability to send phishing en masse or integrate into botnets. And if the account is truly valuable, Steam's outsourced support enters the picture. Fraudsters draw up fake activation keys, write to support, and incompetent (or bribed) employees transfer the expensive inventory to a new address. This gave rise to an entire category of "Recovered Accounts" — profiles that Valve's outsource effectively stole and laundered for criminals.

9. The Myth of Duplication and Shadow Confiscation of Assets

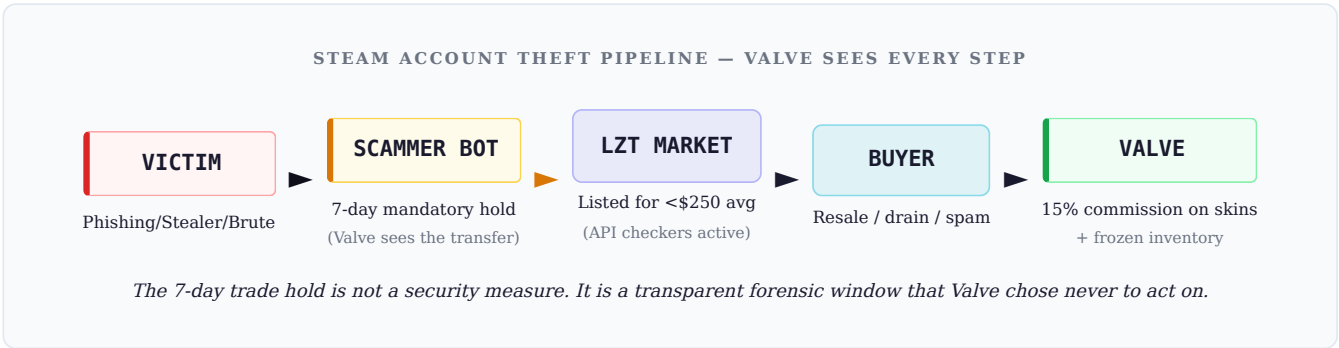


*Diagram **The linear theft pipeline Valve could have disrupted at any step since March 2016.** Every transaction visible in Steam logs. Action was a choice.*

Steam loves to hide behind fighting "duping" (item duplication) to justify refusing to return stolen items. This is a brazen lie. The era of duping ended in 2014. With the introduction of the 7-day trade hold in December 2015 [14] (and its subsequent tightening), the logistics of theft became entirely linear: Victim -> Scammer's bot (7-day hold) -> Shadow market.

Where is the dupe in this? If a scammer deceived a victim and took a rare skin, it sits on the bot. Valve bans that bot. And then what? The item does not return to the victim. It is permanently frozen in the banned bot's inventory. Valve removes the asset from circulation, creating artificial scarcity of rare items, which directly drives up prices on the marketplace and increases the corporation's commission income.

This is not justice. This is shadow confiscation. In financial systems (such as those involving USDT), blocked funds are returned to the legitimate owner through a chargeback mechanism. Steam knows perfectly well how a chargeback works when it comes to topping up their own balance with dubious cards — they block those transactions instantly. But when a user has an item worth $5,000 stolen, Steam washes its hands. They close tickets, threaten account deletion, and refuse to reverse the single fraudulent transaction, proving that their primary objective is to appropriate the asset for themselves.

9a. Forced Blindness: How Valve Hides Hundreds of Millions in Confiscated Assets

THE THREE-LAYER LEGAL ARCHITECTURE — WHY VALVE MADE BANNED INVENTORIES INVISIBLE

1. DESTROYING EVIDENCE FOR CLASS ACTION LAWSUITS

When banned account inventories were public, any attorney could query SteamDB, CSGO.exchange, or Backpack.tf and produce, in seconds, an audited total of assets Valve was holding. That number — **estimated $300M–$500M in frozen user property** — is the foundational figure required to certify a class action. Valve closed this window deliberately. By forcing inventories into a black box, they eliminated the independent financial audit trail that plaintiffs' counsel would need to establish damages at scale.

2. BLOCKING THIRD-PARTY GAME LICENSES — TORTIOUS INTERFERENCE

When Valve bans an account, they revoke access to games from **CD Projekt Red, EA, Ubisoft, and thousands of independent publishers** — games whose licenses the user holds through those publishers, not through Valve. Valve is a distributor and payment gateway in that contractual chain, not a licensor. Revoking a perpetual license issued by a third party — due to a Steam Marketplace dispute — is a textbook case of **Tortious Interference with Contract**. Under EU Consumer Rights Directive, blocking access to paid digital content without refund, where no violation of the specific product occurred, constitutes a direct breach of the user's property rights in the license.

3. THE "PERMANENT" BAN DATABASE TRICK — legal mimicry

Valve does not write "permanent" in the ban database. They write specific dates: 10 years, 25 years, or the 32-bit Unix timestamp overflow — **January 19, 2038**. This is not a technical accident. It is a legal escape hatch.

In civil-law jurisdictions and under EU fundamental rights doctrine, a private company's terms of service **cannot impose permanent, irreversible deprivation of property rights** without judicial review. By calling a 25-year suspension a "long-term service restriction," Valve can claim in court: *"This is a temporary safety measure, not a permanent penalty."* Meanwhile the user is effectively stripped of their account and all licenses for the rest of their natural life. Valve bets that most victims will forget, move on, or not survive the ban window. This is legal gaslighting engineered at the database architecture level.

The Unclaimed Property Question: In most US states and EU member countries, **assets held by a private entity without the owner's access for 3–5+ years must be escheated to the state** under Unclaimed Property Laws. Frozen Steam inventories — held by Valve for years after bans, earning Valve indirect economic benefit through artificial scarcity — may constitute unlawful retention of property that should be escheated. No state regulator has yet demanded an accounting. When they do, Valve's black box will become their biggest liability.

Steam's excuse of "fighting duplication" is dead on arrival. The last confirmed item duplication exploit was patched in 2014. Every ban-and-freeze since then has operated on a linear theft pipeline — Victim → Scammer bot → Market → Valve's frozen inventory — with zero economic justification for permanent asset retention. The only beneficiary of the freeze is Valve itself, through elevated item prices, inflated commissions, and the permanent elimination of any legal accountability for what happened to the property.

THE ABSTRACTISM PRECEDENT (JULY 2018) — DOCUMENTED PROOF THAT VALVE CAN ROLL BACK TRADES

THE SCHEME

Developers under the alias `Kirill_Killer34` paid Steam Direct's $100 publishing fee to upload fake games "Abstractism" and "Climber." They then created items in those games' inventories that were pixel-perfect replicas of the most expensive items in the entire Steam economy: the CS:GO **AWP | Dragon Lore**, Dota 2 **Dragonclaw Hook**, and TF2 **Australium Rocket Launcher**. Thousands of traders saw what appeared to be a Dragon Lore in the trade window. The game name "Climber" was displayed in small print. They handed real, high-value items for empty images from a junk game. The games also contained a hidden Monero cryptominer running silently on victims' machines.

VALVE'S RESPONSE — the golden admission

When the scandal broke on Reddit (*"Steam Direct shovelware developers creating fake TF2, DOTA2, and CS:GO items"*), official Valve developer **Tony Paloma** (`u/Drunken_F00l`) appeared in the thread. Valve removed the games, banned the developers, introduced trade warning banners ("You have never played this game"), and — most importantly — **officially confirmed that victims who lost items prior to the warning banners would have their items returned.** Users confirmed receiving their items back. The rollback happened. At scale. Without breaking the economy.

THE LOGICAL DESTRUCTION OF VALVE'S "TECHNICAL IMPOSSIBILITY" CLAIM

FACT 1 In July 2018, Valve rolled back thousands of fraudulent trades involving Dragon Lore-tier items. The economy did not collapse. No mass duplication occurred. The rollback worked.

FACT 2 Since 2016, when users lose items to API scams, phishing, or infostealer-driven account hijacks, Steam support responds: *"Item restoration is not possible and may result in duplication."*

CONCLUSION **The technical capability exists and has been exercised.** The variable is not technical ability. The variable is **who is at fault.** In 2018, Valve's own moderation process failed (they approved the fake games). Liability exposure was direct and enormous. The rollback function was activated. When API scammers drain your inventory because Valve refuses to patch anomaly detection, Valve is not at fault in their own narrative — so the rollback function stays off. Your Dragon Lore gets frozen. Valve collects 15% when it resells.

Primary source: Reddit thread r/Steam · "Steam Direct shovelware developers creating fake TF2, DOTA2, and CS:GO items" [https://www.reddit.com/r/Steam/comments/9315ju/steam_direct_shovelware_developers_creating_fake/] — official Valve developer confirmation by `u/Drunken_F00l` . Archived. Subpoenable. This is not speculation — it is a documented, on-the-record statement by a named Valve employee confirming that trade reversals are technically possible and were executed. Their current "impossible" position is a provable lie.

THE 100% CONFISCATION MECHANISM — WHY 15% COMMISSION IS THE WRONG NUMBER

STEP 1

Fiat enters Valve's bank

User tops up wallet with real dollars. That money hits Valve's bank account immediately and permanently. Steam wallet funds cannot be withdrawn. **Valve already has 100% of the money.**

STEP 2

Skin = Digital IOU

The item in the inventory is a **digital promissory note**. Valve owes the holder a virtual asset. While it circulates, it retains purchasing power inside the ecosystem. Valve has a liability on their internal ledger.

STEP 3

Ban = Forced Breakage

Ban the account. The digital IOU is destroyed. Valve's internal liability disappears. The real fiat that backed the item? **Already in Valve's bank. Valve keeps 100%.** This is corporate breakage — identical to gift card expiration, but *forced by a unilateral ban*

decision.

THE ARITHMETIC OF 100% CONFISCATION

15% model (what Valve claims):
Scammer sells stolen Dragon Lore on Community Market. Valve collects 15% commission = $300 on a $2,000 skin.
100% model (what actually happens):
Valve bans the scammer bot. Dragon Lore frozen forever. Valve eliminates $2,000 of virtual liability. Original buyer paid real $2,000 in fiat. Valve keeps $2,000. Commission: **100%.**

The 15% Community Market commission is not the profit center. It is noise. The **real engine** is the ban-and-freeze cycle: users inject fiat into Valve's banking system to acquire virtual assets, those assets are destroyed via ban, and the fiat stays. Valve does not care whether a scammer or a legitimate user holds the banned inventory. Banning $100,000 in items erases $100,000 of Valve's virtual liability while leaving the original $100,000 in their bank account. **This is not a security measure. It is unilateral fiat appropriation without judicial process.**

Legal classification: In traditional finance, *breakage income* (unclaimed gift card balances, expired loyalty points) is regulated in most jurisdictions — companies must disclose it and, after a statutory period, often escheat it to the state. Valve's forced breakage via bans is **neither disclosed nor escheated**. It is classified as nothing at all — buried under the catch-all of "ToS enforcement." Under EU accounting directives and US GAAP, undisclosed material breakage income may constitute financial misrepresentation in any public filing. Since Valve is private and files no public financial statements, this liability has accumulated unchallenged for a decade.

INTERACTIVE DEMO: ASSET RECOVERY — TETHER PROTOCOL VS. STEAM PLATFORM

Side-by-side: how Tether restored $10,000 USDT (Bybit hack) vs. how Steam Support responded to an identical theft. Click RUN to simulate both.

10. A Training Ground for Global Scamming

PhishDestroy has been tracking scams since 2018. We know the inner workings. Steam became the primary incubator for cybercriminals. Teenagers aged 14-19 who started with primitive brute-forcing and distributing stealers through fake TeamSpeak servers have grown up. Today those same people use the techniques they refined to attack the Web3 industry (Uniswap) [26] and corporate networks.

Valve raised this generation. Their refusal to punish, their blindness, and their greed showed underage fraudsters that stealing is safe. And the Russian-language outsource, playing at justice and handing out permanent bans without explanation (hiding behind non-disclosure of VAC algorithms), only reinforces this impunity.

14–19

AGE WHEN FIRST
STEAM SCAM LAUNCHED

Web3

WHERE STEAM-TRAINED
CRIMINALS WENT NEXT

0

PROSECUTIONS
STEAM ASSISTED

The career pipeline: Steam phishing → CS:GO inventory theft → infostealer distribution → crypto drain → corporate ransomware. Valve did not just fail to stop this pipeline — they funded its first stage with impunity and frictionless rewards.

10a. The Twitch Contrast: What Happens When a Platform Actually Fights Back

Valve claims fighting phishing at scale is impossible. The comparison with Twitch proves this is a lie.

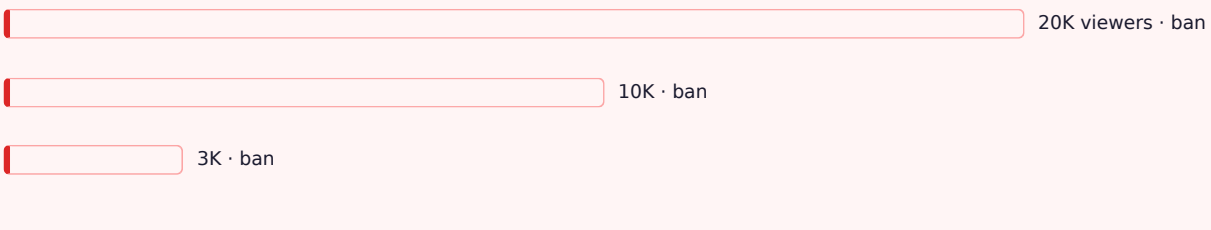
THE TWITCH FAKE STREAM SCAM — AND HOW TWITCH KILLED IT

For a period, Twitch was flooded with fake “Steam skins giveaway” streams impersonating professional esports players — all running **Steam scams and phishing** as their primary payload. Streams accumulated 20,000+ fake viewers via bought traffic. PhishDestroy documented the campaign progression and reported actively.

TWITCH’S RESPONSE (ACTUAL)

- Immediate channel bans when reported
- Proxy pool bans — entire IP ranges blocked
- Algorithm change: sort by engagement, not raw viewer count
- Auto-ban trigger: new account + stream launch + implausible viewer spike
- ~45,000 channels taken down over campaign lifetime
- ~2,000 domains reported and removed

OBSERVABLE DEGRADATION CURVE



Dead

Each successive stream reached fewer viewers before termination. The campaign died from attrition within months.

Critical observation: Twitch was fighting *Steam scams* — not Twitch account theft, not Twitch virtual item fraud. They deployed significant resources — human moderation, auto-ban systems, algorithm changes — to protect their users from a scam that monetized via a *different platform*. Twitch cared enough about their users to fight Steam scams. **Steam never cared enough about their users to fight Steam scams on Steam.**

This comparison destroys the last remaining defense Valve might offer: that the problem is too large and too fast-moving to combat at scale. Twitch proved that determined, targeted platform action degrades and kills sophisticated scam operations within months. Steam has had the same tools, more resources, and direct financial interest in protecting account holders — for over a decade. **The choice not to act was always a choice.**

EPIC GAMES — SECOND EXAMPLE: ACTIVE REAL-TIME BLOCKING

While Valve collects 15% commissions on stolen Steam accounts, Epic Games took the opposite approach. At the time of this investigation, LZT Market displays an active system notification for the Fortnite/Epic Games category: **“Epic Games (partially disabled: account upload and verification may be unavailable)”** — meaning Epic’s backend actively detects and blocks the automated systems LZT uses to validate and list stolen accounts. Epic is not just fighting scammers. It is fighting the infrastructure of the marketplace itself, in real time.

EPIC GAMES’ APPROACH

- Actively blocks LZT Market API account-checker endpoints
- Anti-automation systems detect and disable bulk account validation
- Real-time disabling of stolen account upload pipelines
- Result: Fortnite category on LZT marked “partially disabled”

VALVE’S “APPROACH”

- Steam API remains fully open to LZT Market account checkers
- No rate-limiting on automated bulk validation requests
- No detection of LZT-origin API keys
- Result: Steam is LZT’s largest and most active category

Reference: The infostealer industry’s dependence on gaming credentials is documented in Infostealers.com: “The Future of Cybercrime 2025” [https://www.infostealers.com/article/private-stealing-the-future-infostealers-power-cybercrime-in-2025/] — noting that gaming accounts consistently rank among the highest-value infostealer targets. Epic Games’ active countermeasures demonstrate this is a solvable problem. Valve’s inaction is a policy choice, not a technical constraint.

11. Proof of Convenient Blindness

TIMELINE OF DELIBERATE INACTION — KEY DATES VALVE SAW EVERYTHING AND CHOSE SILENCE

2014
Last confirmed item duplication exploit patched. Trade holds introduced 2015. From this point: **every freeze is theft, not anti-dupe protection.**

2016–2018
Direct links to stolen Steam profiles posted on shadow markets for years. A 10-line script could have flagged compromised accounts. Valve watched. Did nothing.

2018 (ABSTRACTISM)
Valve proves they CAN rollback trades (Dragon Lore scale). The function exists. It is *switched off by policy* when the theft isn’t Valve’s fault.

2024-2026

LZT Market processes millions of stolen accounts. Steam API actively validates them. Valve collects 15% on skin resales. **Deliberate inaction confirmed by 8+ years of documented evidence.**

There is an irrefutable fact proving that Valve deliberately covered for black markets. For years — we emphasize, years — direct, open links to stolen Steam profiles were posted on the pages of shadow markets. Valve needed no complex investigations. A ten-line script could have parsed the market's database once a minute and placed a "Red Tag" (KT) on compromised accounts pending verification by the rightful owner.

This did not happen. Millions of transactions passed under the cover of "convenient blindness." Only recently have the markets begun proxying data (via steam-preview) to hide profiles from independent researchers and bypass privacy settings. But history remembers everything. Valve could have destroyed this market with a single click. Instead, they chose to skim the cream off it.

12. Digital Fingerprinting: Why Proxying Markets Does Not Save Valve

The newest defensive mechanism of shadow markets — proxying links through steam-preview — is used by Valve as yet another convenient excuse for their inaction. The corporation pretends that it is now "harder" for them to identify stolen profiles. This is an absolute lie. For Valve's security systems, an account listed for sale remains as transparent as glass.

Identification via Digital Fingerprint: The market's preview dump openly publishes exact purchase dates and amounts (for example, -2.85 EUR from June 15, 2026), the exact registration date, and balance. In Valve's database, no two accounts with an identical transaction history physically exist. A straightforward SQL query from the support side locates this profile in milliseconds, even if a direct link to it is hidden behind a proxy.

API Anomalies and Interception Patterns: To generate a preview, the shadow market's checker queries the Steam API. On the account itself, a characteristic chain reaction is triggered at that moment: email change, password reset, Steam Guard re-linking, and a simultaneous inventory valuation request, all compressed into a few minutes. All of this happens from the IP addresses of known proxy farms.

DIGITAL FINGERPRINT — WHAT A SINGLE SQL QUERY REVEALS ABOUT AN ACCOUNT LISTED ON LZT

Transaction history
Exact purchase dates + amounts (e.g. −2.85 EUR · Jun 15 2026). No two accounts share identical history. Locates account in milliseconds.

Registration date + balance
Exact creation date + current wallet balance visible in preview dump. Combined with transactions = unique fingerprint.

API anomaly chain
Checker query → email change → password reset → Guard relink → inventory valuation. All from proxy farm IPs. Visible to Valve in real time.

Valve's response
None. The account continues to be listed. Sells. Resells. Valve collects 15% on every skin transaction that follows.

Steam proxying by shadow markets does not defeat this fingerprint. It only removes the direct link. The transaction signature remains fully readable in Valve's own database, accessible to any support employee with a standard query.

13. The Evolution of Interception: From SSFN to Pass-the-Cookie and JWT

Valve's most egregious crime is not the theft of skins. It is their conscious facilitation of the spread of malicious software and the financing of global botnets through vulnerabilities in their own architecture.

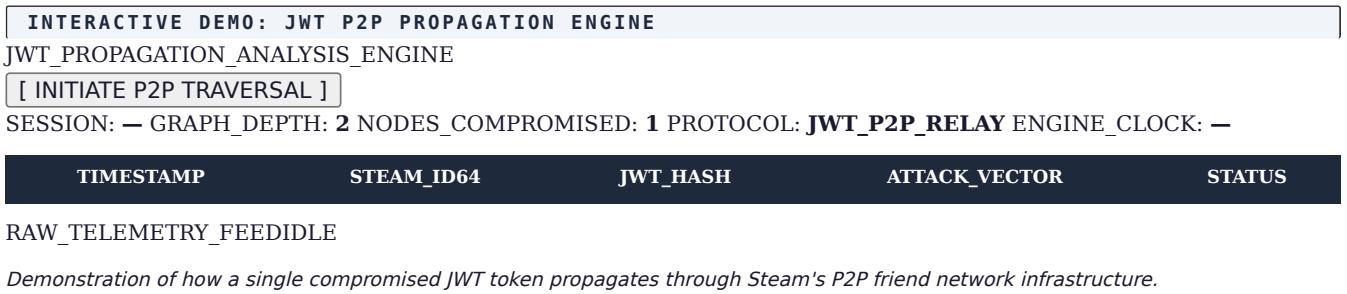
For a long time, the primary vector for session interception was SSFN files [27]. Today the industry has moved forward: attacks have shifted to hijacking web session cookies and JWT tokens (JSON Web Tokens) [21]. The architecture of scamming has become smarter — attackers have learned to validate these tokens locally, without direct requests to

Steam's servers, making such attacks invisible to Valve's primitive anti-fraud systems, assuming those systems are not configured for strict monitoring (and they are not).

The technical mechanics work as follows:

Step 1. Trust Infrastructure as a Free Assembly Line: Since a single stolen token is often insufficient for fully unlinking a protected account, attackers squeeze a different resource from the obtained session — trust. A script gains access to the victim's chats and sends phishing links or virus installers to the entire contact list. Steam graciously provides hackers with its internal P2P infrastructure as a perfect, free engine for the geometric expansion of botnets.

Step 2. Criminal Negligence (Ignoring UEBA): Whether it's an outdated SSFN tied to specific hardware, or modern session cookies — Steam sees 100% of the anomalies. When a token legitimately issued to a PC in, say, Moscow suddenly initiates activity from a German dedicated server, any normal corporation (take Google, for example) would instantly kill the session and issue a red alert: "Session compromised. Your PC is infected with an infostealer." Steam does not do this. They allow the bot to burn through the entire friend list, infecting hundreds of new machines.



Demonstration of how a single compromised JWT token propagates through Steam's P2P friend network infrastructure.

Step 3. Global Damage (Corporate Collapse): This is where the main threat to the entire internet lies. Because Steam does not notify the user of the session interception, the person continues to sit at their compromised computer. If an alert had come, they would immediately wipe the OS. But Steam stays silent. That same person, on that same infected PC, continues to log into their corporate VPN, work email, and crypto wallets.

By ignoring session interception anomalies, Steam is not merely allowing the theft of in-game pixels. They are concealing from the user the fact that an infostealer is running on their system. This corporate blindness directly leads to massive corporate data breaches and infrastructure compromises, with damages running into millions of dollars.

Step 4. Exposing the Lie: The Lawyers' Data

Valve frequently hides behind the claim that they allegedly have "no technical capability" to track complex theft chains, or that "the user is at fault" for the compromise. But the case of the improperly redacted documents from their European lawyers (Taylor Wessing) [9], which we uncovered, proves the opposite.

In the unredacted GDPR request data [10], we clearly saw: Valve logs absolutely everything. They collect deep telemetry on hardware, IP addresses, device change histories, and behavioral patterns. They know the moment an account is hijacked. They see infostealers and spam-sending software running. They have all the tools for automatic blocking and issuing a Red Tag. Their inaction is a conscious corporate choice.

Step 5. Real Motives: Why This Benefits Valve

The lie about "technical impossibility" covers a cold economic calculation.

Support Cost Optimization via Scripts: Blocking a suspicious session means receiving a ticket from a user that needs to be processed. It is more profitable to simply ignore the incident. Steam relies on primitive scripting logic that scammers know perfectly and exploit. Russian-language support staff likely read these algorithms, but not to patch vulnerabilities. Issuing a Red Tag requires no man-hours if the algorithm is properly configured. Previously, a Red Tag could be removed automatically by simulating recovery from a new IP via a VPN. Now, ticket processing times are deliberately dragged out to discourage users from contacting support at all. And a support employee's ability to unilaterally close an unresolved ticket is the pinnacle of corporate cynicism.

The Money Cycle: A hijacked account that has burned through its friend list with spam will eventually receive a VAC ban or community ban. The victim (or their deceived contacts) registers a new account and buys the same games again. The corporation makes double revenue from a single user.

Symbiosis with the Shadow Market: The more accounts are stolen, the faster the gears of LZT Market and other hacker exchanges turn. This shadow activity paradoxically sustains the engagement of a huge audience (especially in regions where the cheat industry flourishes). And any subsequent transaction involving stolen skins still brings Valve their rightful commission percentage.

WHY STEAM IS THE #1 INFOSTEALER TARGET — AND WHY STEAM KNOWS

Steam accounts rank on par with cryptocurrency wallets as the highest-priority targets for infostealer operators — but with one critical difference. A crypto wallet requires the private key. A Steam session cookie requires only the cookie. The Steam session cookie **lives for 200 days and auto-refreshes itself**. No 2FA bypass. No SMS intercept. No brute force. The cookie is the account. If a stealer finds it in the browser profile folder, the account is already gone.

WHY STEAM IS CROWN JEWEL FOR STEALERS

- **200-day auto-renewing cookie** — no re-authentication required
- **SSFN files (legacy) → JWT tokens (current)** — both portable
- **Steam is non-portable by design** — but nobody enforces this
- **Friend network** — stolen account = free spam delivery to 100s of contacts
- **Family PIN** — 4-digit, bruted programmatically in 20–30 seconds
- **Stealer logs** = cookie folder + passwords + autofill + `R code` if found
- **Traffic value** — Steam community + friends = viral phishing vector

WHAT STEAM SEES — AND IGNORES

- New device fingerprint using existing session
- New IP address — often datacenter proxy pool
- Thousands of account-check requests from one IP
- Non-human request patterns (automated pipeline)
- Session active simultaneously from geographically impossible locations

Steam's response to all of the above: nothing. No session kill. No anomaly alert. No email. No push notification. Session stays live.

WHAT WOULD COST STEAM ALMOST NOTHING TO IMPLEMENT

A push notification or email: *"Your Steam account session was accessed from a new device and IP. If this wasn't you, click here to kill all sessions and check your computer for malware."* Microsoft does this for OneDrive. Google does this. Apple does this. Even mid-tier crypto exchanges do this. If Steam sent this alert correctly, at minimum half of active infostealer victims with anything of value on their accounts would be warned in time. Steam has every device fingerprint. Every IP history. Every behavioral log. Building this would take one developer one sprint. **They haven't built it.**

Microsoft

Alerts on new device/IP for OneDrive/Outlook. Session tied to device. Auto-kill on anomaly.

✓ **Protects users**

Epic Games

Actively blocks LZT Market API checkers. Account upload/verification disabled in real time.

✓ **Fights the market**

Steam / Valve

Sees new device, new IP, mass automated requests. No alert. No session kill. No action.

× **Deliberate inaction**

There is also the question of Telegram. If a stolen Telegram session is used from a new device, Telegram's single-session architecture logouts both the attacker and the victim simultaneously — the conflict kills the session. Steam has no such protection. A stolen Steam session coexists with the original indefinitely. The victim never knows.

The 90 million account "leak" (2025): Reports claimed 90 million Steam accounts were exposed via a Twilio SMS gateway. What this actually means: someone registered 90 million accounts using an API-connected SMS service — automated mass registration on throwaway numbers. Valve prohibits automation. Valve prohibits mass registration. Yet 90 million auto-registered accounts existed. Valve counts them in their user statistics. They ban active accounts with real value. They do not ban obvious bot registrations en masse. **The numbers serve the PR. The bans serve the revenue model.**

14. Trading in Lives: What Steam Is Actually Selling for $2

Valve claims to care about privacy. But what does an attacker who has bought a hijacked profile on the market for a couple of dollars actually receive? Steam will not show them the full credit card number, but it will hand over something far more valuable for social engineering.

With an active session (SSFN, cookies, or JWT), a hacker can pull the saved billing address in a few clicks — the victim's real first name, last name, city, and zip code. Through Steam's built-in data panel, they gain access to IP address history and links to other platforms (Twitch, Xbox). And if you look through the support ticket history, you will find archives of unredacted bank receipts and photos of activation keys from physical discs that users sent for verification.

WHAT A $0.08 STEAM ACCOUNT ACTUALLY CONTAINS — BEYOND IN-GAME ITEMS

CHILDREN'S PERSONAL DATA

Real name, last name, home address, postal code — from receipts and support tickets. Minors routinely share home addresses when requesting help with activation keys.

IP ADDRESS HISTORY

Full log of home IP addresses and hardware IDs. Reveals home network, ISP, geolocation. Direct target for spear-phishing and — in conflict zones — physical risk.

PERSONAL PHOTOS & CHATS

Via support tickets: photos of CD keys, receipts, family photos. Private chat archives store years of conversations — links to social accounts, passwords, family details.

CROSS-PLATFORM ACCESS

Steam profile links to Twitch, Xbox, Discord, YouTube. Active JWT session gives access to shared credentials. Infected PC = corporate VPN, email, crypto wallets.

Valve's own GDPR logs confirm they collect all of this. When forced to release data under GDPR Article 15, they handed over hardware fingerprints, IP histories, and behavioral logs — then tried to hide it under a black PDF overlay. Taylor Wessing redacted nothing. The data was fully readable. It was seen by at least 5 parties before the original owner received it.

But the most alarming aspect is the chat logs. We see how Valve has been carefully storing unencrypted archives of personal correspondence for years. In those archives, teenagers leave links to their real social media accounts, share their problems, send passwords for local servers and home IP addresses. By refusing to instantly reset hijacked sessions and by covering for infostealers, Steam effectively puts users' life histories and digital security on display in the windows of shadow markets.

14a. The $1.60 Digital Dossier: How Steam Sells Children's Lives to Shadow Markets

When Valve discusses account security, they talk about inventory value. But the true price of a stolen profile is not measured in pixels. For millions of teenagers, Steam is not a store — it is their primary social network. It holds their achievements, their secrets, their relationships, and their first loves.

When a hacker steals an account and casually dumps it on LZT Market for 150 rubles (approximately $1.60), the buyer does not just receive access to games. **They receive an unencrypted archive of a child's life.**

CHATS, PHOTOS & PRIVATE LIFE

Steam stores gigabytes of personal messages. Teenagers use the in-game client for daily communication — confessions, arguments, life plans. Documented cases on shadow forums show leaked log archives containing minors' personal and intimate photos. Valve does not moderate this content, does not implement end-to-end encryption, and allows hijackers to exfiltrate all of it in a single export.

IP ADDRESSES & PHYSICAL THREAT

When teenagers play together on private servers, they post home IP addresses and open ports directly in Steam chat. This data sits in unencrypted logs for years. For a buyer of a stolen account, this is a ready-made database for DDoS attacks, targeted phishing, home network scanning — or **swatting**. The digital threat becomes physical within minutes.

THE CD-KEY ABSURDITY

When a child loses their social life, Steam support requires a photo of the CD key from a game gifted **10 years ago**. A corporation storing hardware fingerprints, geolocation, and years of behavioral telemetry forces a teenager to dig through a garbage dump for a cardboard box. This is not a security system. It is a mechanism deliberately designed to **legally deny help**.

► **150 rubles ($1.60) on LZT Market buys:** active Steam session • years of private chat logs • home IP address history • linked Twitch/Xbox/Discord accounts • billing city and postal code • friend list (200+ people) • all support ticket history • hardware fingerprint (for credential stuffing against corporate VPNs). **This is not a gaming account. This is a complete personal intelligence file on a minor.**

COPPA VIOLATION — CHILDREN'S ONLINE PRIVACY PROTECTION ACT

$50,000+

FTC PENALTY
PER VIOLATION

<13

AGE THRESHOLD
COPPA COVERS

70M+

ACCOUNTS SOLD
VIA LZT LIFETIME

WHAT COPPA REQUIRES — WHAT STEAM IGNORES

COPPA mandates

- Verifiable parental consent before collecting under-13 data
- Clear data retention and deletion policy
- No sharing of children's PII with third parties without consent
- Data minimization — collect only what is necessary

Steam's actual practice

- IP history, geolocations, hardware fingerprints — logged from day one
- Private chat archives retained for years with no deletion mechanism
- PII shared with outsourced support (Taylor Wessing confirmed)
- JWT session tokens containing user data leak via compromised accounts onto shadow forums

The math the FTC uses: Each individual child's record collected, processed, or transferred without verifiable parental consent is a **separate COPPA violation**, carrying a civil penalty of $50,000 or more. Steam does not verify the age of new users. It does not require parental consent. It stores years of chat logs, IP histories, and behavioral profiles — then allows that data to exit the platform via compromised JWT tokens that land on LZT Market listings for $1.60.

Multiply the FTC math: 70 million accounts sold on LZT over its lifetime. A statistically conservative estimate puts the share of under-13 users at Steam's own reported 10–15% of its playerbase. That is **7–10 million potential COPPA violations**. At $50,000 per count, the civil exposure is **$350 billion to $500 billion** — before GDPR, before state AG actions, before class actions. The number is not real, because enforcement is political. But the liability is structurally there, and Valve has never once conducted a COPPA audit.

16a. Industrial Parsing: Valve's Open API as a Victim Targeting Platform

How did scammers know who to target? How did children become victims at industrial scale? Because Valve left the doors of their database wide open.

THE HATLER ERA — STEAM API AS AN INDUSTRIAL VICTIM SCANNER

For years, shadow market operators used specialized software (including tools like **Hatler**) to parse Steam users at industrial scale through Valve's open API. Scammers configured filters the way a retail platform configures product searches:

Filter: Group members. Parse all members of a specific gaming community. Target fans of a popular streamer.

Filter: Inventory value. Find all users with open inventories containing CS:GO Covert-tier items or Dota 2 Arcanas.

Filter: Online status. Find all users currently active. Optimal phishing window: *right now.*

Brute-force fallback. When group-based targeting was insufficient, scanners brute-forced SteamID ranges: **20 million IDs at a time**, through cheap public proxies. Valve saw no problem with this.

THE BOTNET MACHINE — 300,000 BOTS, MILLIONS OF MESSAGES, ZERO ACTION

300K

BOTS PER
ACTIVE FARM

10-30K

BOTS PER SINGLE OPERATOR

M/day

IDENTICAL PHISHING MESSAGES SENT

Valve claims to have “advanced algorithms.” How does an advanced algorithm fail to detect 300,000 accounts sending millions of *identical messages* to the same targets, at the same time, from the same proxy ranges, every single day? **It doesn’t fail. It ignores.** All real damage to phishing infrastructure was done by independent projects like PhishDestroy — not by the multi-billion-dollar corporation with a bloated security department that was supposed to protect the children on its platform. **Valve didn’t protect children. It provided scammers with a convenient API to find them.**

15. "Efficiency" Built on Children's Tears: The Business Model of Total Indifference

THE REAL COST OF VALVE’S “EFFICIENCY”

What Valve saved

- ~$500M/year in security staff not hired
- ~$200M/year in anti-fraud infrastructure
- ~$100M/year in support quality
- Highest profit-per-employee in gaming

What users paid

- 75–100M accounts stolen via LZT over lifetime
- $450M+ estimated minimum victim liability
- Millions of infected PCs (infostealer spread)
- Children’s PII on darknet forums

Valve’s **profit-per-employee genius** was purchased at the cost of systematically denying help to millions of children who lost real money, real data, and real safety. This is not optimization. It is **profit extracted from victims.**

Valve loves to boast about its financial analytics: hundreds of millions of dollars in profit per a couple dozen store employees. In the eyes of the tech industry, Gabe Newell often appears as a genius of optimization. But let's take off the rose-tinted glasses and call things what they are: this "efficiency" was purchased at the price of an absolute, cynical refusal to ensure the security of their own users.

Unlike public companies (such as Roblox or Tencent), whose market capitalization instantly collapses at the slightest scandal around child safety or data breaches, private Valve is accountable to no one. They have no board of directors. They do not need to reassure institutional investors. They have built an ideal printing press where the absence of spending on Trust & Safety and anti-fraud departments converts directly into personal billions for management.

The price of this "hyper-optimization" is millions of hijacked accounts, personal correspondence of teenagers leaked to the internet, a thriving shadow market, and complete impunity for scammers. Valve is not merely "failing to notice" fraudsters. It is economically beneficial for them to do nothing about it.

16. Steam API: A Corporate Toolkit for Hackers

STEAM API — DESIGNED FOR SECURITY, USED FOR MASS THEFT

Millions

LZT API CALLS/DAY VALIDATING STOLEN ACCOUNTS

$0

COST TO ABUSE
THE OFFICIAL API

0

BOTS BANNED FOR
API ABUSE IN 2024

79

STAFF WATCHING
ALL OF THIS HAPPEN

Let's dissect Valve's lie about their alleged inability to control theft. If they wanted to, any support employee could go to a shadow market, take a link to a listed Steam account, and look in their own server logs at exactly which API key and from which IP address is right now evaluating that profile's inventory to generate a dump on the forum.

Valve would see a network of proxies and hundreds of API keys. Most of them have likely been obtained from previously stolen accounts. What should the corporation do? Revoke the compromised keys. But Steam does not do this. Why? Possibly because they fear catching "legitimate" services in the net — roulettes, illegal case-opening casinos, or third-party marketplaces where pixels are exchanged for crypto without AML procedures. This entire ecosystem exists in a gray zone, generating massive traffic while not being taxed. And Valve is entirely fine with that.

Steam's Terms of Service explicitly prohibit any automation. A reasonable question then arises: why does the official Steam API contain functions that are ideal for the automated hijacking of accounts (which takes milliseconds) or the mass linking of mobile authenticators?

Why does Steam allow virtual (VoIP) numbers from SMS activation services to be mass-linked to accounts? The solution for filtering such numbers is trivial — standard HLR lookups used by any normal service. But Steam does not do this. Perhaps, in the pursuit of impressive "record online" figures they love to brag about, bot farms are advantageous to them?

When a user receives a VAC ban [15] for cheating, the ban hits all accounts tied to the same phone number. But when hundreds of accounts are hijacked from a specific pool of VoIP numbers — Valve does not ban those numbers. Any normal service (Telegram, Netflix, Apple, Google) blocks junk or compromised phone numbers. But for Valve, security is an empty word.

17. Willful Blindness: A Legal Shield Made of Hypocrisy

FIVE LEGAL VECTORS FOR VALVE ACCOUNTABILITY

Vector 1: OFAC Sanctions Violations & Money Laundering

Direct transactions and wallet top-ups from sanctioned territories (Crimea, DNR, LNR) continuing since 2021. Use of sanctioned gateways (Tinkoff Bank) via shadow intermediaries and region-switching. ToS self-certification clauses are legally void — Valve collects full hardware telemetry and traffic routing, meaning they practice **Willful Blindness** as defined under OFAC doctrine.

Targets: DOJ NSD · OFAC · FATF

Vector 2: Complicity in Infostealer Distribution (CISA / IC3)

No immediate JWT/cookie session invalidation on anomalous geo-change. Steam's P2P infrastructure (chats, friend lists) used as botnet expansion engine. A $2 stolen log caused a corporate lockdown, $17M ransom, $100M+ total damage. Valve's silence is the enabling mechanism.

Targets: CISA · IC3/FBI

Vector 3: GDPR Violations — PII Disclosure of Minors

Taylor Wessing's improperly redacted GDPR DSAR response disclosed third-party PII including minors. Fines reach 4% of global revenue. Elite lawyers billing €1,500/hr leaking data in official responses proves the Data Protection Officer function is operationally nonexistent inside Valve.

Targets: EU DPAs (CNIL, BfDI, AP, DPC)

Vector 3b: COPPA Violations — Children's Online Privacy Protection Act (FTC)

Steam collects IP addresses, hardware fingerprints, geolocations, and private chat logs from users under 13 without verifiable parental consent — a direct COPPA violation. Compromised JWT tokens carrying this data exit the platform onto shadow forums. Each individual record = $50,000+ in FTC civil penalties. 70M+ accounts sold on LZT, 10–15% estimated under-13, yields theoretical exposure of $350B–$500B before state AG enforcement and class actions.

Targets: FTC (COPPA Rule) · State AGs · DOJ Consumer Protection

---

Vector 4: Corporate Fraud & Fictitious ToS (FTC / SEC)

Steam ToS prohibits all automation. The Steam API simultaneously processes millions of daily requests from LZT Market checkers validating stolen accounts. 79 employees for 500M users is mathematical proof security was never budgeted. Frozen inventory on banned bots (Shadow Confiscation) proves bans serve Valve's economy, not justice.

Targets: FTC (Section 5 UDAP) · SEC

Vector 5: Internal Corruption & Unregulated Virtual Currency

Support agents used system privileges to duplicate Dragon Lore/Dota couriers and fence them via Chinese exchanges. Sold trade-ban removals for crypto bribes. Steam Wallet and skin economy function as unregulated virtual currency serving criminal syndicates without KYC/AML. Forensic analysis links support staff crypto wallets to 100% AML-flagged addresses.

Targets: FinCEN · DOJ Criminal Division

THE WASHINGTON SHIELD & THE MOSCOW BOW: VALVE'S LEGAL SCHIZOPHRENIA

For 99% of the planet, Valve has built an impenetrable legal fortress: "All disputes shall be maintained exclusively in King County, Washington, U.S.A." — the perfect shield against their own users.

But the final clause reads: **"If you are a consumer who lives in Russia, you may also seek a remedy with local Russian state courts."**

Out of 195 countries, Valve makes an exclusive legal carve-out for the Russian Federation — a state under the heaviest international sanctions in modern history.

Crimea, DNR, and LNR are, per the Russian constitution, serviced by "local Russian state courts." If a resident of these occupied, sanctioned territories sues Valve in such a court — does Valve comply?

If YES

Valve recognizes the annexation and commits a direct OFAC sanctions violation.

If NO

Valve violates its own ToS and defrauds users — breaking the Russian laws it so desperately appeases.

> *Checkmate, Taylor Wessing. You drafted a rule that makes you either liars or accomplices to international sanctions evasion. Pick your poison.*

*OFAC**Sanctions breach categories documented by PhishDestroy in this investigation.***

Valve created an ecosystem where violating the rules (automation, VPN use, farming, bot-running) is a basic condition of the platform's survival. They hand hackers a perfect toolkit (open API), turn a blind eye to virtual numbers, but carefully keep in the rules a strict prohibition of all of the above.

This is not mere negligence. This is deliberate blindness (Willful Blindness / Deliberate Ignorance), constructed as a perfect legal shield. When a regulator comes to Valve, lawyers like Taylor Wessing [9] will show the ToS: "Look, we prohibit everything!" And when a robbed teenager comes to them, they use that same ToS to legally deny them help and avoid spending time on an investigation.

18. The Symbiosis of Intelligence Services, Steam, and Hacker Markets

Let's return to LZT Market. We have already established that Steam does not care at all about this platform. But another aspect is interesting. Over the course of its existence, this shadow forum has survived at least three changes in management, which, by indirect (but very obvious) indicators, are connected with the redistribution of spheres of influence among certain echelons of power in the Russian Federation.

During periods of management change (for example, during the era of the administrator Thomas), radical purges took place on the forum. Fraud schemes targeting Russian residents were banned (Avito scam, anti-cinema), the leaking of intimate photos of minors with personal data was strictly suppressed, the sale of VKontakte accounts was completely removed, and currently the sale of Telegram accounts registered on Russian numbers is prohibited. The forum is clearly moderated to avoid touching Russian citizens in ways that are critical.

But the situation with Steam is different. The market still freely sells Steam accounts belonging to Russian citizens who were infected by stealers. The listing description directly states: origin — stealer, country — Russia, balance — in rubles. This means that a Russian user caught a virus that drained not only their Steam but also, very likely, their email accounts and work credentials. And the forum passes this through without issue.

The question arises: does Steam cooperate with the same structures that oversee this market? Or perhaps Valve could influence their "partners" in Russia to stop the double standards and ban the sale of stolen accounts belonging to Russian citizens? Because right now Steam and the shadow market are operating in perfect symbiosis, as if they copied each other's policy of double standards and hypocrisy.

STEAM'S DOUBLE STANDARD — BANNING ANTI-WAR CONTENT WHILE HOSTING RUSSIAN STATE PROPAGANDA

BANNED BY STEAM MODERATION

- Comments calling Russia's invasion a war
- Posts referring to Russian forces as aggressors
- Content supporting Ukrainian resistance
- Any "political statements" in community hubs

APPROVED AND MONETIZED BY STEAM

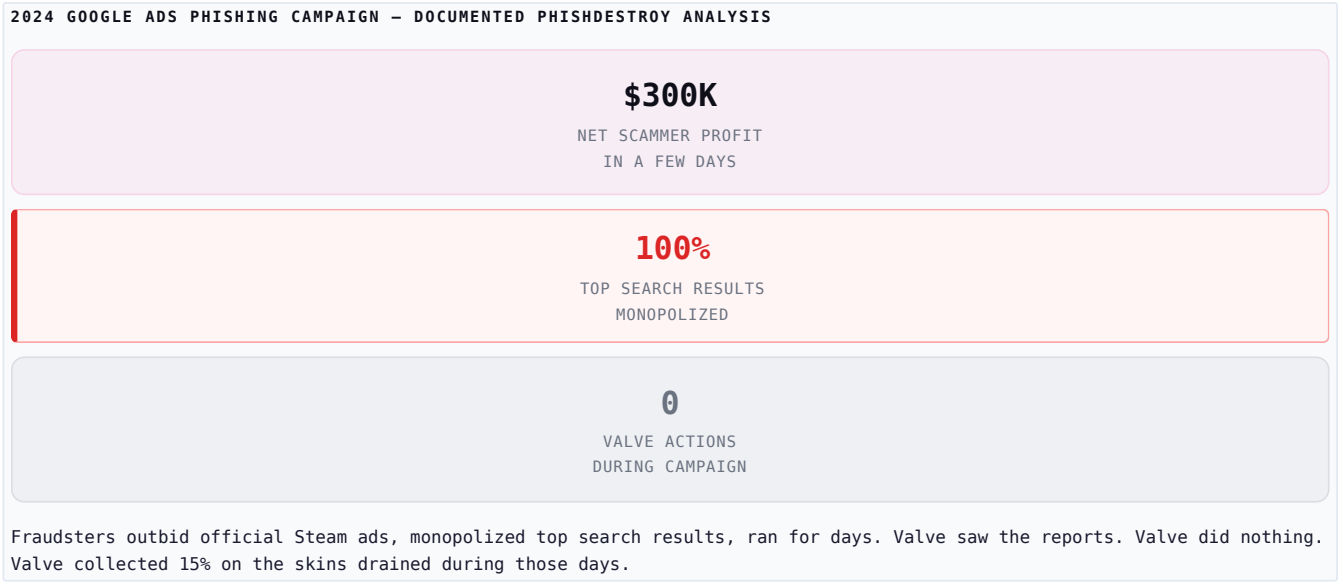
- Purchasable "Putin & Trump" profile backgrounds
- Thousands of "Putin forever," "Putin smile" items
- Sanctions bypass tutorials in official Guides
- Region-switching instructions for OFAC-banned zones

Steam did not draw these images. But it **distributes, lists, and monetizes** them through a Valve-operated marketplace — while aggressively scrubbing any content that names the perpetrators. This is not accidental moderation. It is **political curation in favor of the Russian state.**

19. The Anatomy of Scamming: From Fake Windows to $300,000 Net Profit via Google Ads

Over the past 5-8 years, PhishDestroy has dissected virtually every scam scheme in the Steam ecosystem. We have seen infostealers that substituted authentication windows on the fly, intercepted SMS messages, and wiped inventories clean. We have seen the mechanics of trade offer substitution (API Scam) that remained "unnoticed" by Valve for years. Unnoticed — or too profitable?

We conducted continuous analytics on the bots of the largest phishing networks. Here is an example: in 2024, we recorded a massive pour via Google Ads [29]. Fraudsters substituted the displayed URL in ads with the original Steam domains. The purchasing was so aggressive that it outbid official advertising, monopolizing the top search results.



By our calculations, in just a few days of continuous operation, the scammers' net income amounted to approximately $300,000. And that is accounting for the discount when selling stolen skins on shadow markets and the tiny, cosmetic bans that Steam occasionally handed out. Yes, these are peak figures driven by the economics of that period, but the fact remains: Steam is an enormous feeding trough.

And while phishing is almost exclusively interested in CS and Dota (rather than other games), Rocket League, Path of Exile, Rust, and PUBG should not be forgotten. But here, Valve's corporate extortion enters the picture: strict NDA (Non-Disclosure Agreement) conditions that all developers are required to sign. A developer is not permitted to publicly disclose security issues, data breaches, or vulnerabilities in Steam without Valve's written approval. Even if this directly threatens their players. Mouths are sealed by contract.

20. The BlockBlasters Case: A Month of Blindness and the Lie About a "Hacked Developer"

The BlockBlasters case is not about ignoring pixel theft — it is about concealing actual criminal offenses.

Recall the recent incident with the game BlockBlasters [5], which only received public attention thanks to the late streamer Raivo Plavnieks [6]. This was a targeted attack on influencers: fraudsters contacted streamers, bought advertising, and asked them to launch the game directly from Steam. The victims' logic was understandable and fatal: "It's the official Valve store — there can't be an outright stealer in there." How wrong they were.

Steam support began receiving reports with ironclad evidence as early as September 2nd. The tickets contained ChainAbuse [7] complaints about stolen cryptocurrency and direct evidence of the scammers' open Telegram API embedded directly in the game's code. What did Valve do? It waited. For a month. The stealer games were peacefully downloaded from the store.

And then the corporation rolled out an excuse that insults the intelligence of any security professional: "The developer's account was hacked." Let's call this fairy tale what it is — a brazen lie to cover their own negligence (or complicity).

To release a game, a developer is required to pass Steam Direct KYC [22]: pay $100, submit their real name, address, and banking and tax details. The perpetrator was not an anonymous hacker from the dark web — their legal information, including a W-8BEN tax form [8], was sitting in Valve's database.

The myth of a "hacked developer who for some reason stayed silent for 22 days" collapses against the architecture of Steamworks. When a legitimate developer loses access to the publisher console, they create a ticket about stolen credentials. Publication rights for updates and builds are frozen within hours.

Only two options remain. Either the "developer" was originally a co-conspirator of the fraudsters (meaning Valve's vaunted KYC is a fiction). Or Valve deliberately ignored, for an entire month, the desperate attempts by the developer and dozens of robbed victims to reach support, while malware stealing crypto was being distributed through their official store.

In both cases, Valve is acting not as a victim of circumstance, but as the primary accomplice in a digital robbery.

21. Destroying Evidence: How Valve Cleaned Up the Crime Scene

But the most disgusting part of the BlockBlasters case is the ending. Interference with a digital crime scene.

On the record: Valve did not delete the infected game. Our forensic analysis of the C2 infrastructure proves the opposite. The scammers themselves deleted the malicious builds from Steam's servers on September 21st — precisely when their Telegram botnets were publicly exposed and criminal charges were becoming a real possibility. They applied a scorched-earth tactic to cover their tracks.

Valve's statement about "security measures taken" is pure fiction and shameless PR. They deliberately waited for the criminals to erase the malware from their own servers, and only then leisurely removed the now-empty store page, claiming credit for themselves. This is not solving a problem. This is complicity and obstruction of justice.

Valve was not protecting users. It was cleaning up the crime scene so that federal agents with a court order for distributing infostealers through their own data centers would not show up at their offices.

THE BLOCKBLASTERS COVER-UP — DOCUMENTED SEQUENCE OF EVENTS

SEP 2	**Reports filed.** ChainAbuse complaints + Telegram C2 key visible in game code. Ironclad evidence submitted to Steam support.
SEP 2–21	**22 days of silence.** Malware freely distributed via official Steam Store. Valve staff read the tickets. Took no action.
SEP 21	**Scammers self-clean.** After their Telegram C2 was publicly exposed, fraudsters deleted all malicious builds themselves. *Valve did not remove anything.*
OCTOBER	**Valve “acts.”** Empty store page removed. Press release issued claiming security action. **The crime scene had already been cleaned by the criminals.**

> Developer KYC data (W-8BEN tax form, real name, billing address) sat in Valve’s database for 22 days. They never cross-referenced it with the complaint evidence. The evidence for federal prosecution was in their own system the entire time.

22. The Illusion of Action: Restricting Limits to Save Server Costs

When Valve does introduce some restrictions (for example, cutting friend-request limits), naive users think it is out of security concern. Nonsense. This whole story about limits is not about fighting scams — it's about plain and simple savings on server capacity.

Let's recall what started the spam apocalypse. Before the famous trade offer substitution script appeared, the platform was being abused by primitive automation. Armies of bots with female avatars were sending phishing links by the thousands. This junk traffic created enormous demand for no-limit accounts. We were tracking shadow markets: due to this spam boom, the price of a stolen account without a spending limit shot up from 25 rubles to a stable 150. And this insane demand for stolen profiles persisted right up to 2024!

THE LIMIT CUT PROOF — SERVER COST, NOT USER SAFETY

> **IF IT WERE SECURITY:**

Freshly registered throwaway accounts (the ones spammers used) would have had limits cut first. Instead, Valve cut limits on fully-developed, no-limit accounts — the most valuable ones for bot operators.

WHAT ACTUALLY HAPPENED:

Millions of identical invite/cancel transactions were generating database writes. Server costs spiked. Valve cut the limits to **protect their infrastructure**, then called it an "anti-spam measure."

Do you think Steam cut the invite limit from 100 to 30 to protect you from phishing? Think again. Valve logs everything: every click, every invite, every cancelled request. The automated scammer farms were generating millions of empty transactions per day, polluting Steam's internal databases and overloading the infrastructure. And what is most telling — Valve did not crush these limits on freshly registered throwaway accounts, but on fully developed no-limit accounts (including those with a VAC ban, since they technically count as accounts that have crossed the spending threshold). Valve cut the limits solely to reduce the load on their own servers, not for your safety.

Restrictions at Valve only appear where they need to protect their own servers. Your money is none of their concern.

THE BAN REASON LIE — WHY VALVE NEVER EXPLAINS COMMUNITY BANS

WHAT VALVE CLAIMS

"We cannot disclose ban reasons to protect the integrity of our anti-cheat systems." A reasonable-sounding excuse — for a *VAC ban*. Community Bans and Support closures have nothing to do with anti-cheat.

THE ACTUAL REASON

If Valve disclosed ban reasons, they would need to legally justify *why they now own your items*. They cannot. The frozen inventory is legally theirs only if no one challenges it. Silence is their legal shield — not security policy.

The calculation is deliberate: 95% of victims are minors who will not hire lawyers, cannot navigate Washington State courts, and accept "ToS violation" as a final verdict. Valve architected their legal system specifically for this audience. The ban reason policy is not about anti-cheat — it is about keeping children compliant.

23. The Inner Workings: Why Scammer Supervisors Benefit from Bans

Since we have dissected scam teams from the inside, I will expose one dirty secret that ordinary traffers never even suspected.

In all scam teams (where rank-and-file workers are promised 90-95% of stolen inventory), the supervisors (team coordinators) had a financial incentive to get a trade ban or Red Tag placed on their bots. Therefore, they deliberately did not replace compromised bots. If an account received a ban, the supervisor's share shot up sharply: instead of a measly 5% from the skin sale, they received between 15% and 20% of Steam's price for the inventory (not the market price!), simply by selling banned accounts with valuable skins to the Asian market. Chinese buyers purchased them in bulk to play with expensive items and private cheats. This is why a huge number of accounts with trade bans also carry VAC bans. The scam industry was feeding the cheat industry, and Steam was happily collecting the online numbers.

24. Steam Workshop: A Perfect Testing Ground for API Scam

Steam's absolute disregard for security is well illustrated by the Workshop incident. At some point, literally 2-5 scammers completely flooded the Workshop with phishing ads. How? They used intercepted web sessions of real users.

This was not a hijacking in the classical sense. The attacker simply opened a parallel session on your account via the Steam API, scanned the inventory, waited for you to initiate a trade, instantly cancelled it, and substituted an identical offer (with the same avatar and friend nickname) from their own controlled bot. All of this happened within a legitimate user session through official Steam endpoints.

And what did Valve do when the Workshop was drowning in phishing? They did intervene, of course. They issued Red Tags and banned the compromised accounts... but did so only after the inventories of those victims had been completely wiped clean.

Excellent work, Steam. Thank you for "saving" the account when there was nothing left in it to save.

Ironically, the price of these tokens on the black market has collapsed. If previously a valid SSFN file could go for around $3, today on that very LZT Market (where the curator of Russian-language Steam support, Nikita, is registered) the price list looks like a mockery of Valve's security:

> *"Buying and processing Steam Tokens (JWT). Fast check with proprietary software. Prices:*

$0.08
CS2 PRIME JWT TOKEN

This is the market price for a valid CS2 Prime session token on LZT Market. For eight cents, an attacker gets an active Steam session, access to the victim’s friend list, chat history, billing region, IP log, and the ability to send phishing to every contact.

CS2 Prime — $0.08 (no temporary or permanent bans)

OpenTM — $0.04 (open trading platform)"

Your account, your history, and your data are valued at 8 cents. That is all you need to know about the effectiveness of session protection in Steam.

The Illusion of "Technical Impossibility": The Fake Games Case

Support claims that returning stolen items is "technically impossible" or would "destroy the economy." The game spoofing incident proves otherwise.

The scheme was brazen: scammers uploaded dummy games to the Steam Store, creating items with names and icons copied one-to-one from expensive CS:GO and Dota 2 skins. During a trade, the victim saw a familiar Dragon Lore, completely unaware it belonged to a fake game. We remember this perfectly, as PhishDestroy was actively hunting and blocking these scammers at the time.

And what did Valve do when the very foundation of trust in the Community Market was threatened? A miracle occurred. The corporation, which for years had refused to help phishing victims, suddenly returned the real items to all affected users. The scammers were hit with such a carpet bombing that they howled on shadow forums for days: Valve issued hardware bans (HWID) and blanket-banned shared IPs so harshly that entire scam syndicates went deep into the red.

Moreover, Steam rolled out a massive security update in a matter of days. Suddenly, they found the resources to implement everything: trade holds, new verifications, developer deposits, massive red alerts stating "This game has never been played by you," and warnings about suspicious disparities in item values.

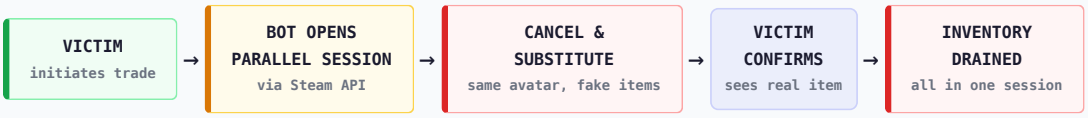
It turns out they can. They know perfectly well how to track transaction chains, roll back trades, and build a complex warning architecture. But they only do it when they feel a direct threat to their own business model and the credibility of their marketplace. If you are stripped naked by a standard stealer, you will simply receive a boilerplate reply that "Steam policy does not provide for item restoration."

79 Employees: An Architecture of Matches and Acorns

To fully grasp the "seriousness" of the platform's day-to-day security, consider the recent API bug that lived in production for two whole days. Anyone with a basic script could send a simple request and spam system notifications directly to absolutely any Steam ID, completely bypassing all privacy settings.

Two days of a gaping hole in the API allowing anyone to ping millions of users. Indeed, 79 employees for a multi-billion-dollar global platform is clearly enough. Why invest in a functional QA and security department when you can just write a Terms of Service agreement that blames the user for everything?

API TRADE SUBSTITUTION MECHANICS — HOW STEAM’S OWN INFRASTRUCTURE ENABLES THE SCAM



Every step uses official Steam API endpoints. The parallel session is opened through legitimate Steamworks calls. Valve could detect the pattern — two simultaneous sessions on the same account, one initiating and one cancelling identical trades. They did not patch this for years.

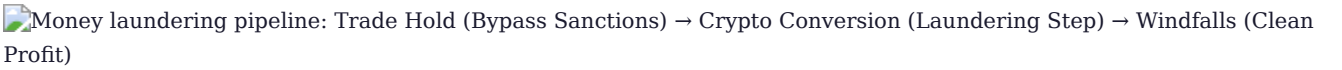
25. Infrastructure as a Service: Scam-as-a-Service (SaaS)

To give you a sense of the scale of commercialization spawned by Valve's inaction, look at a typical offer from a modern phishing team. These are no longer teenagers with broken scripts. This is a full-fledged SaaS business with fierce competition. While we were mercilessly blocking their domains and forcing them to lose money on infrastructure, they switched to providing free domains to their "workers" to maintain volume:

> *"Our project combines 3 in 1: Phishing (logs go to you), MaFile (5% commission), Substitution (API Scam — 80% to you). Only we offer: Auto-sale of logs on LZT, MaFile removal with a single code, Browser for substitution, Free domains and a multitude of fake templates."*

Valve only fixes what becomes uncontrollable, or what affects geolocations they are afraid to disturb (USA, Japan, South Korea). Steam could see the spam, see the no-limit accounts, and sometimes even banned phishing domains (often when they were already dead). If the corporation saw a domain, it also saw the network of accounts distributing that domain. Given that the farms operated through cheap shared proxies (using the scheme of 1 server and 100 IPs per 1,000 accounts), blocking the entire botnet could have been done with a single SQL query. But Valve did not do it.

26. Geopolitical Hypocrisy: The Steam Economy Laundromat



*Flow**Stolen Steam skins used as anonymous currency: sanctions bypass → crypto conversion → clean profit.**Valve takes 15% at each transfer step. No KYC. No AML. No enforcement.*

Valve's tolerance for the gray CIS economy spawned yet another monster — the market for illegal balance top-ups and region-switching. When Valve officially closed direct top-ups for Russia, it simply turned a blind eye to the flourishing of shadow intermediaries. Much more convenient that way, right?

The "region-switching" service (to Turkey, Kazakhstan, or Argentina) was sold by the millions. On just one platform (like FunPay) [24], more than 500,000 transactions have been recorded from several large sellers. And there are hundreds more Telegram bots and forums. This top-up industry has become deeply intertwined with the laundering of money from phishing and crypto scams (the buying up of seed phrases).

What is Valve's logic? Do they genuinely believe in the mass migration of millions of teenagers from a sanctioned country? Or do Russian funds, passed through a Kazakhstani proxy and a stolen inventory, simply "smell different"? Valve does not care about sanctions and compliance. The main thing is that a 30% commission from every transaction reliably drips into their bank accounts, while lawyers churn out boilerplate letters about the "impossibility of technical intervention."

27. Corporate Benefit and Violation of Their Own ToS

Steam is an ecosystem that thrives on total violation of its own rules, and Valve knows this perfectly well. The Terms of Service (ToS) clearly state: extracting any commercial benefit on the platform is strictly prohibited.

Now let's look at reality. Selling stolen accounts, skin trading, bot farms for farming collectible cards, Level Up services (profile leveling), selling keys, and of course, balance top-up services for sanctioned regions. All of this is direct commercial benefit. And this is surreal: a platform that formally prohibits commerce is home to industries with multi-million turnovers. Valve (or their reliably NDA-protected Russian-language outsource) has abstracted itself from its own rules, applying them exclusively as a tool to punish those who fall out of favor or to protect infrastructure.

SELECTIVE ENFORCEMENT — THE TOS VALVE ENFORCES VS. THE VIOLATIONS IT PERMITS AT SCALE

AGGRESSIVELY ENFORCED

- User publishes anti-war comment
- User asks for item return after theft
- User appeals a permanent ban
- Developer mentions security vulnerability

NEVER ENFORCED (ToS violations)

- Millions of automation bots (ToS §prohibited)
- 500K+ commercial account resale listings
- Gambling sites built on Steam API
- Sanctions bypass via region-switching services

28. The Support Syndicate: Why Valve Cancelled Item Returns

Diagram ***The documented support corruption chain: admin access → mass item duplication → black-market fencing via crypto bribes.*** *This is not a hypothetical. PhishDestroy documented cases where support staff used system privileges to duplicate Dragon Lore and rare Dota 2 couriers, then fence them through Chinese exchanges for crypto. Valve abolished item returns to stop this — but punished users, not the corrupt staff.*

When Valve justifies its refusal to return stolen items to users (hiding behind fighting inflation or "duping"), they are blatantly lying. The reason Valve permanently freezes assets on banned bots, pocketing them into their bottomless account, is not protection of the economy. It is an attempt to recoup operational losses inflicted on them by their own employees.

Historical fact: support agents (including cheap outsourced workers often mistaken for volunteers) were directly integrated into the shadow economy of Steam. Using their system privileges, they turned technical support into a corrupt cartel.

Industrial Duplication of High-Tier Items: Support employees were mass-generating copies of the most expensive items in the game (Dragon Lore in CS:GO, rare Legacy couriers in Dota 2) under the pretext of "returning stolen inventory to a user." This "returned" inventory was then fenced on Chinese exchanges for real money.

Selling Unbans: Support was selling the removal of Red Tags (KTs) and trade bans from the profiles of major scammers. For bribes (in crypto or skins), fraudsters were given the green light to cash out assets worth tens of thousands of dollars.

Upon learning the scale of the corruption, Valve's management was furious. They permanently abolished the policy of returning stolen items, cutting support's manual access to item generation. But those punished were not the corrupt employees — it was the users. Children and gamers around the world are paying with their money for Valve's failure to control its own staff.

The "Little Tyrant" Syndrome and the Fall of the Volunteer Police

In addition to official support, Steam had a second branch of power — a volunteer trade police integrated with databases like SteamRep [12]. They held enormous informal influence over the platform's economy and the fates of traders. And they turned out to be no better than the outsourced staff.

The volunteers devolved into a closed, corrupt caste of "faceless shadow authorities." They suffered from a classic "little tyrant" syndrome: they buried traders they disliked, banned users who discussed vulnerabilities, and issued "free passes" to friends.

When logs surfaced proving that SteamRep [12] admins were taking bribes to remove "scammer" labels and were running cover for massive bot networks laundering stolen skins, Valve's trust collapsed completely. By 2022, Valve had expelled the last volunteer moderators, replacing them with rigidly scripted outsourced workers.

THE UNREPORTED CRIME — EU AML LAW AND VALVE'S ILLEGAL SILENCE

THE CEVA LEAK — WHY VALVE DISCLOSED IT

The recent EU user data breach was disclosed not because Valve chose transparency, but because CEVA Logistics — a compliant public company — was legally required to report the incident. Valve was forced into an unusually public situation. Had Valve directly controlled the leak, they would never have notified users — just as they did not notify the 1,000+ victims whose data PhishDestroy documented.

RUSSIAN OUTSOURCE: NO REGIONAL LIMITS

Right now, the Russian-language outsource support contractors have unrestricted global access to every Steam account — with zero geographic filtering. They can view *any* account: IP address history, billing region, linked email, transaction logs. There is no technical or policy barrier preventing them from querying the account of any individual — private citizen or public figure — anywhere on the planet.

THE QUESTION VALVE REFUSES TO ANSWER — EU ANTI-MONEY LAUNDERING LAW

When Valve's outsourced support staff (operating through Ireland) stole inventories worth **€100,000–300,000+** from users — and Valve quietly replaced the contractor without telling anyone — did Valve file a **Suspicious Activity Report** with the relevant EU Financial Intelligence Unit? Did they report the theft to the Irish Gardaí Síochána or the relevant national authority?

Under EU law (AMLD6), proceeds from theft above €10,000 that circulate without being reported constitute money laundering. Steam skins — which have a documented, liquid, exchange-rate-linked market value and are directly convertible to fiat through shadow exchanges — are functionally a currency. When support staff drain an inventory worth €150,000 in skins and those skins enter the underground trading ecosystem, those are **criminal proceeds circulating in the European financial system**. Unreported. Untaxed. Untraced.

Valve's implicit argument: "Skins are not money, so we are not obligated to report." But the EU's AMLD framework applies to *assets of value*, not just fiat currency. The European Banking Authority has repeatedly stated that virtual assets with exchange value fall under AML obligations. By the time stolen Steam skins converted to crypto bribes on Chinese exchanges fund the next cycle of support corruption, they have passed through multiple European financial jurisdictions. **Valve made this choice deliberately.** Informing regulators would expose the systemic nature of the problem. Staying silent allowed them to change a vendor and move on.

29. The Price of "Efficiency"

THE FINAL TALLY — WHAT A DECADE OF DELIBERATE BLINDNESS COST THE WORLD

70M+
STOLEN ACCOUNTS
VIA LZT (LIFETIME)

$450M+
MINIMUM VICTIM
LIABILITY

8+
YEARS OF
DOCUMENTED BLINDNESS

5
LEGAL VECTORS
FOR ACCOUNTABILITY

$0

VALVE FINES
PAID TO DATE

Valve boasts the highest profit per employee in the industry. But what is the cost of this profit?

This efficiency is built on denying help. On threatening phishing victims. On closing tickets. On suppressing the truth that Steam is not so much a gaming platform as a global crypto laundromat and distribution hub for infostealers.

While Valve's management considers itself geniuses of business optimization, fighting in court for the right to sell adult visual novels, their platform is daily chewing through the data, money, and safety of real users. The era of duping has long been dead, but Valve continues to use it as an excuse to legally appropriate the property of robbed users. There is no justice in Steam. There are only scripts, outsourced workers, and an endless thirst for profit.

30. Hypocrisy at Every Level: The Corporate Ethics of Valve and Taylor Wessing

If it seems to you that mentioning Taylor Wessing in the context of their internal harassment lawsuits is a joke — **it is not.** A firm whose partners demonstrated a documented willingness to protect abusers internally is the firm Valve chose to stonewall the GDPR rights of children. The pattern is consistent. The choice was deliberate.

If it seems to you that I am exaggerating by mentioning Taylor Wessing (Valve's lawyers) in the context of their internal harassment lawsuits — believe me, it is not a joke. The court case was lost, but the point is not the verdict — it is Taylor Wessing's strategy. They demonstrated not professionalism, but a dirty game of attrition and deliberate delay. Google how many years the case dragged on from the time of the incident at the elite ski resort.

But when it comes to Valve itself, even more questions arise about their vaunted ethics. They have a corporate Welcome Book where they call themselves a "family." All warm and cozy. But when this "family" is rocked by scandal, Valve acts with maximum ruthlessness. Recall the harassment of a transgender employee in support, or the story of Jess Cliffe [13] (the co-creator of Counter-Strike, who had worked at Valve almost since its founding). The man was thrown out of the company without a court verdict, on the basis of accusations alone. Valve, which generates millions by covering up scams, suddenly became afraid for its reputation? The logic is absurd: a company allows millions of dollars to be stolen from its users but instantly distances itself from the person who built this business for decades, just to appear "clean."

As for the lawyers at Taylor Wessing — let's be honest. You pride yourselves on your "centuries-long history," but on your Instagram, you are running a race in support of Pride. Make up your mind: do you honor the history of your Nazi founders who sent gay people to concentration camps, or are you a modern progressive company? This is corporate scamming. You want to appear as ancient aristocracy while having effectively merged into the ecstasy of contemporary hypocrisy. And yes, you have taken on the defense of Russian oligarchs in cases where your reputation was openly screaming: "You are not hired where people are innocent."

31. The Roadmap of Coming Leaks: What Valve Should Prepare For

This is not the first and not the last piece from PhishDestroy about Valve. I will not play cat and mouse with their lawyers — their time, judging by their rates, costs $3,000-$5,000 for reading a couple of paragraphs. Don't waste the money; hire decent support staff instead of a Russian outsource that reads from scripts.

Here is what comes next. My roadmap for upcoming investigations:

Evidence Base on GDPR Impotence: I will publish the originals of the legal boilerplate letters and improperly redacted documents, proving that Valve systematically violates regulations and discloses the confidential data of underage users. I will show the entire chain in which I was already the fifth person to have gained access to someone else's personal data (including individuals with Russian passports). This is direct proof of their lies about storage conditions and mythical "encryption."

NDA Violation and the Dirty Underbelly of Steamworks: We have data from at least two developers whose non-disclosure agreements (NDAs) we will be happy to violate (we never signed them). We will expose the open chaos in update moderation and cases involving locker content that Valve prohibits from being made public under threat of game removal.

Crypto Failures and Money Laundering: How Valve's "Geniuses" Lose Their Millions: Since Valve loves to brag about the billion-dollar profits of their employees, we, as PhishDestroy, will venture into crypto territory. We will conduct a forensic financial analysis of the wallets belonging to elite support staff (early Bitcoin investors) and show how these "professionals," bringing Valve billions on the tears of robbed children, themselves invested in scams and had their addresses flagged with 100% AML risk scores.

The Strange Love of Russia and Who Is "Nikita": We will examine the phenomenon of Valve's tolerance for the CIS region. How does a person with no formal employment become a support supervisor simply because they once created a fan community for Half-Life? We will expose the loopholes and sanctions bypass mechanisms for developers from a terrorist state, as well as direct balance top-ups from the DNR/LNR and Crimea that have been functioning since 2021 and continue to this day.

PART II

GDPR Stonewalling

Originals of Taylor Wessing’s improperly redacted documents. Full chain of 5+ data recipients. Minors’ PII visible under the black overlay.

PART II

Crypto Wallet Forensics

Support staff wallets — early Bitcoin investors with 100% AML-flagged addresses. How scam proceeds funded the people protecting the scam.

PART II

Who is “Nikita”

How a person with no formal employment became a support supervisor. The loopholes. The NDA violations. The account movement from one contractor to the next.

PART II

Steamworks NDA Violations

Data from two developers whose NDAs we never signed. Open chaos in update moderation. Content Valve prohibits publishing — published here.

32. Conclusion

I have no desire to dedicate my life to writing texts about Steam. It is run by an audience of children, scammers, and Putin cultists on the platform (in the form of the Russian outsource). Volunteers are mired in corruption up to their ears. If Gabe Newell considers himself a genius of the gaming industry, then perhaps it is my destiny to be the bastard who writes the truth into history:

Gabe is an excessively petty and greedy monopolist who legalized the theft of money from children. And the promised private jets and vacations from their employee handbook are just colorful pictures designed to keep workers in corporate bondage.

All of this is written for history. For the Web Archive. And for those regulators who will eventually come to dismantle this empire of impunity.

33. Anatomy of the ToS: Corporate Schizophrenia and Legal Cynicism

Let's dissect Steam's Terms of Service (ToS). We will cover at least 25% of this document to show that this is not a legal contract — it is a lie constructed to allow the platform to steal from children while avoiding accountability.

Here is a quote from their rules: "You may not use any scripts, bots, macros or other automated systems ('Automation') to interact with Content and Services on Steam..."

We will analyze this clause in detail in the next part. Spoiler: Steam itself created an API that is used exclusively for automating theft, bypassing limits, and managing bot farms. The platform wrote a rule that it simultaneously allows to be violated on an industrial scale.

And here is another gem of corporate cynicism: "You acknowledge that Valve is not required to provide you with notice prior to terminating your Subscription and/or Account."

This is a lie. Under normal legislation, that is not how it works. But the platform shields itself from everything. Valve's position sounds like this: "We steal from children, we violate sanctions, we allow infostealers to infect your PCs, but if anything — you are at fault, and we will take your account without explanation."

They love to say that "the community decides everything." But for some reason, when it comes to legal accountability, the community suddenly becomes a powerless piece of meat.

KEY TOS CLAUSE — THE AUTOMATION PROHIBITION THAT ENABLES THE THEFT

> *"You may not use any scripts, bots, macros or other automated systems ('Automation') to interact with Content and Services on Steam..."* — Steam Subscriber Agreement

The **same platform** that bans automation simultaneously exposes an official public API that processes millions of automated requests daily from LZT Market account checkers, inventory validators, session hijackers, and card-farming bots. This ToS clause is not a security measure. It is a **legal escape hatch** — when a regulator points to the mass automation, Valve can show the rule. When a robbed teenager asks for help, Valve shows the same rule to deny the claim. One document. Two purposes. Zero enforcement against profitable violators.

34. Sanctions, Terrorism, and Double Standards

A funny question for this corporate hypocrite. The rules state: "If you are a consumer residing in Russia, you can also seek legal protection in local Russian state courts."

Does the court of annexed Crimea count as a Russian court? Or shall we wait for Roskomnadzor — with which Steam integrates so cozily — to answer?

And here is a clause that provokes a roar of laughter: "You agree to comply with all applicable import/export laws and regulations. You agree not to export Content... to any countries that support terrorists... You represent that you are not in such a prohibited country."

So when Valve accepts money directly from accounts registered in zones subject to international sanctions (and we have gigabytes of screenshots and direct proof of transactions from Crimea, the DNR, and LNR dating back to 2021) — it is not Valve violating sanctions. It is the user's fault! The platform quietly edited its ToS over the last six months, shifting all responsibility onto users.

Valve, were you compelled to remove mentions of Russia's allies (Cuba, Iran, Syria) and prohibited from speaking ill of them, or did you calculate the scale and the sum that came directly from those places? If a terrorist state is coercing you into any actions — tell someone, do not be afraid. There is no need to violate current US law because of threats that they will pirate your content; it is not worth that risk. They are terrorists, and you are a US company. If you are being persecuted or blackmailed, contact the FBI Seattle Field Office at +1 (206) 622-0460 [16] or IC3 [17]. I am also confident that specialists from CISA [18] could help you: given the scale and reach of your sphere of influence, it is significant even by US standards.

Since you are removing direct sanctions rules and changing the text — this is a very alarming signal. I am not joking: if you do not trust the agencies named above, then here you will certainly receive help at the highest level — at DOJ NSD [19]. We, for our part, will conduct additional analysis and free consultations with certain specialists, and may also be compelled to report this where appropriate (or nowhere). But this is no joke at all — it is serious.

You removed explicitly enumerated countries from the rules and shifted responsibility onto users. At the same time, you run analytics: there is a tracking pixel on the registration page, and you see the real number of clicks through to the agreement. Nobody reads it, because you have calculatingly disguised it as a question confirming that the user is over 13 years old (the link to the agreement is embedded there as well). Modern society — children and teenagers — has ADHD, and this is a scientifically proven fact: check the data. They do not finish reading text. I, for example, saw the clause about being over 13 and that was it — I looked no further. This is direct manipulation on your part, as is the rewriting of the agreement regarding countries that have consistently appeared on sanctions lists.

Your revision directly indicates that your company's attitude toward those countries (or money from them) has changed. This is a very strange change. Most likely, there is already a problem, or you are complying with Russian courts, and this is one of their non-public demands — such as the banning of certain users, etc., which could undermine belief in the

rightness of their terrorist acts on the territory of another country. Or are you simply prostrating yourselves before the Russian government, fulfilling their direct requests to ban undesirable users? I will show you prior versions of your ToS. You may change them as you wish, but these pieces of paper are worthless when it comes to the direct violation of US laws and the sponsoring of terrorist economies.

35. Blackmail and the Scorched-Earth Strategy

Fair warning in advance: any attempts by Valve or their attack dogs from Taylor Wessing [9] to make contact will be treated as pressure and obstruction of the investigation.

Do not try to send us an NDA. PhishDestroy is not registered on your garbage heap. We did not check the box in your clever agreement (which you treat exclusively as confirmation that a child is over 13 years old, so that you can legally rob them).

If your lawyers try to accuse us of "extorting billions of rubles" or "defaming the holy reputation in the interests of a North Korean competitor, Steam 2.0" — good luck. All of our investigations, evidence, and proof are duplicated to independent nodes (including servers at an American university) and the Web Archive. This is not a conflict. This is a statement of facts.

DEAD MAN'S SWITCH — IPFS ACTIVATION CONDITIONS

If Steam, Taylor Wessing, or any affiliated entity attempts aggressive action against this project, the response is not legal — it is technical: **full raw data dump to IPFS.** All evidence, all communications, all unredacted documents. The domain dies. The data lives forever at **steamdestroy.eth**. No seizure. No injunction. No takedown. The content-addressed file system does not have a registrar.

36. The Scam Factory: Carding, Fake Documentation, and Data Theft

You think scamming on Steam is only about stolen passwords? You have no idea of the real scale.

Fake Documentation (Social Engineering): When an account is stolen, support demands the first CD key from 10 years ago. The child doesn't have it. But the scammer from Russian outsource does. Fraudsters commission the fabrication of fake receipts and keys on shadow forums. We have collected over 200+ proven instances of successful fakes that Valve's support staff happily "swallowed," handing the account over to criminals.

Data Theft: More than half a million accounts (including EU citizens) have passed through the shadow market LZT. Steam concealed the fact that their PCs had been infected with stealers. The platform de facto leaked to hackers personal data, correspondence, IP addresses, and home network information.

Industrial Carding: If Valve's lawyers understood how carding works on their platform, their hair would turn white. Issuing a Red Tag for carding while leaving items purchased with stolen credit cards on the account is a remarkable money laundering practice. Do you know who was actually competing with the Prince of Saudi Arabia for the highest Compendium level in Dota 2? We will tell you about that too.

200+

PROVEN FAKE CD-KEY
SUBMISSIONS ACCEPTED

500K+

EU CITIZEN ACCOUNTS
THROUGH SHADOW MARKET

15%

VALVE COMMISSION ON
EVERY RESOLD STOLEN SKIN

36a. The Gambling Machine: How Valve Built the World’s Largest Unregulated Casino for Children

Skin gambling is not a side effect of Steam. It is a **predictable and profitable** consequence of Valve’s deliberate architecture: open trading API, no KYC, virtual items with stable secondary market value, and complete regulatory blindness. The result: a $1B+ annual industry where children’s CS2 skins function as casino chips — without age verification, without parental consent, and without Valve ever filing a single SAR.

$1B+

ANNUAL SKIN GAMBLING VOLUME AT PEAK

15%

VALVE COMMISSION ON EVERY SKIN DEPOSITED

0

AGE VERIFICATIONS REQUIRED BY STEAM

THE MECHANISM — HOW CHILDREN’S SKINS BECOME CASINO CHIPS

1
Child earns CS2 skin (in-game drop)

2
Skin has real market value (Steam API)

3
Gambling site accepts skin as deposit

4
Child loses. Site keeps skin.

5
Valve earned 15% at every skin transfer

No step in this chain required Valve to act. The Steam API was the **enabling infrastructure**. The skin economy was the **currency layer**. Valve designed both, monetized both, and filed no SAR, made no age-gate, sent no warning to parents.

The 2023 Bot Ban: Not a Punishment. A Profit Mechanism.

In 2023, Valve banned tens of thousands of bot accounts operated by gambling sites — CSGOFast, CSGORoll, Stake.com (for skins), and others. The gaming press celebrated this as Valve “cracking down” on gambling. This interpretation is **factually wrong**.

THE 2023 BOT BAN — WHO ACTUALLY PAID

WHAT CASINOS LOST

- Bot accounts — new ones spun up within days
- Temporary disruption to automated deposit flows
- **Net financial loss: near zero.** They migrated to new methods.

WHO ACTUALLY PAID

- Children whose skins were **inside the bots at the time of the ban**
- Inventories confiscated by Valve — not returned to original owners
- Valve kept every skin in every banned bot: **Breakage Income**
- The child who deposited their AWP | Dragon Lore as a gambling stake: **got nothing back**

The math: Tens of thousands of bot accounts. Each holding hundreds to thousands of skins. Combined inventory value: tens of millions of dollars. **Valve banned the bots and kept every skin.** The gambling sites paid nothing. The casino operators paid nothing. The children who made the deposits paid everything. And Valve collected their standard 15% commission on every skin's journey through this entire chain before confiscating the final balance.

REGULATORY POSITION: FTC / UK GAMBLING COMMISSION / EU COMMISSION

Steam operated for years as the **settlement infrastructure** for an unregulated gambling ecosystem targeting minors — earning commission at every step and confiscating balances upon "enforcement." Under US law (UIGEA + FTC Section 5), facilitating gambling transactions without age verification and without filing SARs constitutes potential criminal exposure. The UK Gambling Commission has jurisdiction over any gambling product accessible to UK residents. The EU's Digital Services Act requires platforms to prevent illegal content — including illegal gambling advertising and underage gambling access — from reaching minors.

37. Epilogue: A Training Ground for Cybercrime

VALVE'S LEGACY: PRIMARY INCUBATOR OF GLOBAL CYBERCRIME

#1
GAMING TARGET
FOR INFOSTEALERS

$100M+
CORPORATE DAMAGE
FROM ONE $2 LOG

8+ yrs
DOCUMENTED
DELIBERATE INACTION

Steam accounts are the top gaming query for malware operators globally. Without the financial return Steam's shadow market provides, large-scale infostealer distribution campaigns would be economically unviable. **Valve did not build a platform that got exploited by criminals. Valve built the economic engine that made the infostealer industry profitable.**

Since, according to Valve's perverse logic, virtual items "have no real value," the theft of $10,000 worth of skins is not legally theft. This is a perfect gray zone.

But Steam is not merely ignoring theft. Steam has raised an entire generation of cybercriminals. Today's creators of infostealers and crypto scammers started out stealing inventories in CS:GO. Gabe Newell's platform became the primary incubator for global cybercrime, teaching underage hackers the main rule: you can steal on the internet with impunity, as long as you pay the corporation's commission.

Everyone will answer for their actions. Even if they hide behind a Terms of Service they wrote themselves. Expect part two.

38. Sanctions, Censorship, and Steam's Stockholm Syndrome

EVIDENCE: SANCTIONS BYPASS OPENLY HOSTED ON STEAM SERVERS

These are not dark web links. These are discussions and official Guides hosted on Valve's own servers, indexed by Google and Bing, publicly accessible to non-logged-in users. Valve moderates this platform. Every post is reviewed. None of these were removed.

OFAC Violations — Crimea, DNR, LNR Top-Ups

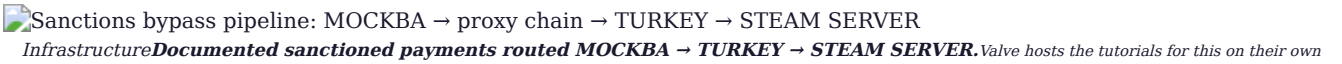
- How to top up Steam in Crimea, LNR, DNR regions [https://steamcommunity.com/discussions/forum/1/592889900452284230/]
- Top-up from Crimea [https://steamcommunity.com/discussions/forum/26/601891815092687488/]
- Top-up in LNR and new territories [https://steamcommunity.com/discussions/forum/26/4691154153116861492/]
- Topping up Steam via Tinkoff (sanctioned bank) [https://steamcommunity.com/discussions/forum/26/3802778195613939203/]

Official Steam Guides — Sanctions Evasion Tutorials

- Guide: How to top up Steam from Russia [https://steamcommunity.com/sharedfiles/filedetails/?id=2933353476]
- Guide: Top up Steam with minimum commission [https://steamcommunity.com/sharedfiles/filedetails/?id=3507230272]
- Guide: Steam Wallet Top-Up Methods [https://steamcommunity.com/sharedfiles/filedetails/?id=2798029444]

Schrödinger's VPN: Valve's Selective Enforcement

Steam ToS explicitly bans VPN use. At the same time, Steam's own servers host thousands of guides on how to change region via VPN. Under **FTC Section 5 (UDAP)** this is a deceptive practice. Under **Estoppel doctrine**, Valve has waived the right to enforce this clause after systematically ignoring it for years — meaning they cannot selectively apply it to deny help to theft victims while allowing bot networks to run freely. Under **OFAC Willful Blindness doctrine**, hosting and indexing this content is not passive — it is facilitation.



*Infrastructure**Documented sanctioned payments routed MOCKBA → TURKEY → STEAM SERVER.** Valve hosts the tutorials for this on their own servers. Nothing was removed.*

Steam's hypocrisy reaches its apex when the subject turns to geopolitics. You may laugh at the fact that a corporate monster generating billions has simply gotten confused in its own algorithms. But let's look at the facts.

In 2022, as the sanctions noose began to tighten, developers from Russia rushed en masse to bypass the blocks. And where did they find the most detailed guides on evading international OFAC sanctions? Right inside Steam itself. In the official Community, there are step-by-step instructions on how to use a VPN (which is formally prohibited by the ToS) to change regions and withdraw money to sanctioned banks (such as Tinkoff Bank) [25].

Here is a quote from an official (or, at least, Valve-moderated) guide that perfectly describes their position: "We kindly ask you to maintain professionalism and refrain from commenting on political matters... Such statements will be removed, and the most active violators will lose the ability to leave comments..."

Translate from corporate speak into plain language: Valve prohibits calling the war a war. Valve prohibits calling the aggressor country a terrorist. Aggressive moderation (hello, Russian-language outsource) scrubs any criticism, protecting an audience that is killing people in a neighboring country from "political disputes." This is not mere negligence. This is complicity in censorship, driven by fear of losing revenue from the CIS market.

I formally invite Valve's management and their vaunted lawyers to come to Mariupol or Melitopol, to see from what exactly "political disputes" they are so carefully shielding their Russian-language community.

EXHIBIT A — STEAM'S OWN SERVERS HOST THESE DISCUSSIONS (CLICK TO EXPAND — NOT THE DARK WEB)

39. Sanctions Bypass as a Platform Service

Steam states that users are obligated to comply with US export laws. But at the same time, the platform serves as the primary hub for publishing manuals on how to bypass them. The guides have been up for years. Switching region to Kazakhstan or Turkey to bypass blocks has become not just a widespread phenomenon, but an industry standard that Valve silently approves.

Why? Because Steam's policy goes like this: "The user ticked the box saying they are not a terrorist and are not under sanctions, so there are no claims against us."

But we will go further. If anyone has raw analytical user databases from Steam, we are ready to put them to work. We will find lists of accounts that have bypassed blocks to purchase games from publishers who officially withdrew from Russia (such as the creators of STALKER 2 [30] or GTA [30]). We will pass this data directly to those publishers, along with the question: "Are you aware that Steam is sabotaging your exit from the market and openly providing users with loopholes to purchase your games in rubles through a chain of intermediaries?"

We already have contacts with insiders bound by NDA. We know of a case where Valve unilaterally terminated cooperation with a developer and simply appropriated their money, covering it with a non-disclosure agreement. But we did not sign any NDA. We will tell everything.

40. Where Are the US Regulators Looking?

The main question: does Valve understand what OFAC [20] (the US Office of Foreign Assets Control) is?

When a platform allows mass sanctions evasion via VPN (from minor purchases to fund withdrawals by developers); when it allows money laundering through shadow skin markets while turning a blind eye; when the platform's moderation integrates Roskomnadzor [23] restrictions and removes "undesirable" posts — this is no longer the jurisdiction of a terms of service agreement. This is the territory of direct violation of US sovereignty and laws.

Expect the continuation. PhishDestroy will not stop until this architecture of lies collapses. All proof and links are saved. And no Taylor Wessing [9] will intimidate us.

Given all these factors, our recommendation is simple: do not yield to Steam's legal framing. If a user is an actual terrorist, they are under no obligation to testify against themselves. It is Steam's absolute legal duty to verify the origin of these funds, rather than granting the user the absurd privilege to self-certify whether they are a terrorist or not. This logic applies directly to Valve's territorial operations. If Valve has suddenly forgotten how the internet works — and its direct bans on VPNs — let's follow their logic: a terrorist from Crimea, Cuba, or Syria goes online to launder money. This user does not know English and has zero intention of reading the convoluted legal nonsense in the user agreement. But they are definitely over 13 years old (in fact, they might have already killed 13 people). Does the platform seriously think it can shift the legal liability onto the terrorist to decide their own status? By shifting this responsibility, Valve is making a direct legal statement: they automatically recognize everyone as a "non-terrorist" on their end. Meanwhile, the actual terrorist, who completely ignores the boilerplate text disguised as a simple age check, simply launders their money using a sanctions-bypass guide hosted directly on Steam's own community platform. Outstanding compliance, isn't it?

Are you out of your minds? You fed the personal data of minors to a person with a grievance, essentially saying, "Here is the cause of your problems, fetch." If that individual ever acts on that data, the blood and legal responsibility rest entirely on the hands of Valve and Taylor Wessing.

The IPFS Dead Man's Switch

We have vastly more information than what is published here. If Steam, Taylor Wessing, or any affiliated entity attempts to take aggressive action against our project, we will not waste time in court. We will execute a full, raw data dump on the InterPlanetary File System (IPFS).

Yes, releasing unredacted data will have consequences. Yes, it will mean the absolute death of the phishdestroy.io domain and its massive traffic. Let us save your lawyers some time: We do not care. The domain was created as a joke to mock the Steam scammers who claimed we "didn't even have a website." We do not chase reputation, we are not trying to be corporate heroes, and we are not afraid to lose a URL.

If the domain dies, you will find the answers at: steamdestroy.eth

Who We Are

PhishDestroy is a non-commercial anti-fraud operation. There are four of us — certified cybersecurity professionals operating across multiple countries. One of our original five members is deceased; that is why you will never find all of us.

40a. Open Disclosure Protocol: Formal Notice to Valve Corporation

`OPEN DISCLOSURE PROTOCOL — PHISHDESTROY · AUGUST 2026`

PhishDestroy does not enter closed settlements, sign NDAs, or engage in corporate extortion. Our objective is transparency and technical truth. This investigation — including raw (de-identified) telemetry, vulnerability reproduction scripts, and blockchain transaction analytics — is published as an open repository. We simultaneously issue this formal open letter to Valve Corporation’s management and legal department requesting clarification on documented technical and legal paradoxes.

VERIFICATION PROTOCOL — all communications are cryptographically witnessed

Pre-publication
Every outgoing request is uploaded to our open repository before being sent.

PGP-signed .eml
All outgoing requests and incoming responses are published in .eml format and cryptographically verified with PGP signatures.

Willful Blindness Doctrine
Letters are sent to all corporate, legal, and public email addresses simultaneously — establishing confirmed receipt.

THREE QUESTIONS REQUIRING A TECHNICALLY AND LEGALLY SUBSTANTIATED PUBLIC RESPONSE:

QUESTION 1: Shadow Asset Confiscation & Anti-Cheat Absurdity

Valve systematically conceals the real reasons for Community bans and inventory freezes behind boilerplate claiming “we cannot disclose anti-cheat (VAC) algorithms.” This is technical and legal nonsense: VAC has no relation to trade lockdowns. Our estimate puts assets illegally held on banned bot accounts (Breakage Income) at $300–500M. **What is the actual volume of currently frozen inventory? Why are owners of confiscated property denied the right to know the real, itemized reason for the block without irrelevant references to anti-cheat?**

PHISHDESTROY COUNTER-EVIDENCE

PhishDestroy maintains independent tracking analytics on publicly known bot accounts and documented threat actors operating on LZT Market. Our data shows approximately **90% of known Steam scammers remain unbanned** — not because detection is technically difficult, but because banning them would eliminate a revenue stream. The “we cannot reveal anti-cheat algorithms” response is not a limitation. It is a legal shield. We are capable of revealing the real methods: the vast majority of CIS scammers on Steam are documented, publicly operating, with years of transaction history. Valve does not lack the data. **Valve lacks the motivation.**

QUESTION 2: The Automation Paradox & Shadow Market Facilitation

Steam ToS categorically prohibits all automation. Reality proves the opposite: Valve created and maintains an API used exclusively for theft. Shadow markets generate millions of API requests daily validating stolen JWT/SSFN sessions. Our telemetry shows 300,000-bot farms, frictionless auto-registration via VoIP numbers, proxy/Tor parsing availability, and

millions of identical phishing messages daily. Time from token theft to dark-market listing: milliseconds. **Why does the official Steam API function as a criminal pipeline while Valve ignores 100% provable industrial automation?**

QUESTION 3: Legalizing Sanctions Bypass (Schrödinger's VPN)

Steam ToS explicitly prohibits VPN use for bypassing regional restrictions. However, on official Steam Community domains — moderated by Valve employees — thousands of guides on region-switching and wallet top-ups (including OFAC-sanctioned territories) have been posted for years and are indexed by Google and Bing. **Is providing Steam servers to host sanctions-bypass guides an official company position, and why is the VPN prohibition enforced exclusively when it benefits Valve?**

ESCALATION PROTOCOL — Regulatory Forwarding on Non-Response

We acknowledge Valve Corporation's right to silence. However, in the legal environment, the absence of responses to documented technical evidence is treated as **Tacit Admission**. Upon expiration of the responsible disclosure window, materials from our repository will be addressed to the following regulators:

OFAC + DOJ NSD
Crimea/DNR/LNR transactions, Willful Blindness, hosted sanctions-bypass guides

FinCEN + IRS
Unlicensed MSB, shadow confiscation as unreported income, KYC/AML failure

FTC (COPPA)
Under-13 data collection, JWT leaks of minors' PII to dark markets, $50K/violation exposure

CISA + IC3/FBI
Steam P2P as free infostealer/botnet engine attacking US corporate networks

EU DPAs
Taylor Wessing GDPR DSAR — improperly redacted documents disclosing minors' PII

Publishers
CD Projekt Red, EA, Ubisoft — Tortious Interference via VPN/region-switching facilitation

The repository is open. The evidence is verifiable. Every move is recorded. If Valve chooses not to speak with independent researchers, this dialogue will be continued by regulators, media, and institutional partners who will ask the same questions in a courtroom. We are waiting for your response.

REPORT TO YOUR LOCAL AUTHORITIES

PhishDestroy is actively seeking countries and regulators for whom it is *not* a matter of indifference that their citizens — and their children — are having their property stolen, are being systematically cultivated into gambling addiction, and are being exposed to what may be, at minimum through Valve's tacit approval, a documented vector for device compromise at scale.

Choose your country to see verified official reporting routes. Nothing is sent automatically — review every fact and submit through the official route yourself.

CHOOSE YOUR COUNTRY

— Select country —

Nothing is sent automatically. PhishDestroy provides verified reporting contacts only. Submit the complaint yourself through the official route.

41. The Ultimatum & Deterrence Framework

IPFS DEAD MAN'S SWITCH — DETERRENCE ARCHITECTURE

We anticipate attempts to apply legal pressure: Cease & Desist, NDA threats, domain seizure. The domain phishdestroy.io is operationally irrelevant. In the event of any legal action targeting researchers or infrastructure, the Open Disclosure Protocol automatically publishes a complete unedited raw data archive to the IPFS network.

ACCESS KEY

steamdestroy.eth

ENS-registered, blockchain-anchored

JURISDICTION

None

DMCA does not reach the blockchain.

Archive contents: Sanctions-bypass transaction logs with routing data; unredacted GDPR DSAR outputs including third-party PII; identifiers of shadow market administrators; AML-flagged cryptocurrency wallets connected to Valve support personnel; API telemetry of validated stolen sessions against Steam endpoints.

A decentralized file system does not recognize Washington State court orders. You cannot serve a DMCA notice to a content-addressed hash.

One question requires a public answer on the record: According to Valve's Terms of Service, does a court in the annexed territory of Crimea qualify as "any local Russian state court"? Without a direct, public answer to this question, do not contact us.

If a "peaceful settlement" is what you want, enforce your own rules:

Ban every account that has ever used a VPN to access Steam (you have the database).

Block every account that has used automation on the platform, including CSGOFast.

Admit that Valve or its proxies conducted a cyberattack against Source 1.

The minimum standard of fairness: return every asset stolen through trade substitution (API scam). Start with every account ever listed on Lolzteam Market. We understand your architecture — we saw your internal device identification logic in those unredacted GDPR documents. "Technically impossible" is not an answer. If your staff cannot do it, replace them. The outcome does not change regardless of what you try. We have no money to seize, no names to expose, and no corporate reputation to ruin. We are armed only with the truth.

A Global Warning: The Infostealer Epidemic and Corporate Collateral

I am addressing every country on Planet Earth — except the terrorist states, since Steam is already getting along with them just fine.

If you care at all that an unaccountable corporation has decided it has the right to steal your children's digital property, listen closely. If you care that they deliberately fail to notify users about infected devices — thereby compromising critical corporate networks worldwide — then pay attention.

In Part 2 of our investigation, we will present a perfect example of what Steam's negligence has actually spawned. We will provide hard evidence proving that Steam is the primary economic fuel for the global infostealer industry. Steam accounts are the top gaming query for malware operators. Without the financial return provided by Steam's thriving shadow market, these massive, indiscriminate infostealer distribution campaigns would simply be economically unviable.

There is already a public case on the record where a $2 stolen log resulted in a corporate lockdown, a $17 million ransom payout, and total damages exceeding $100 million. Thank you, Valve, for your unparalleled commitment to global "security."

We will not hide this intelligence. Information flows to us naturally, and we will publish it all. And let this be our official declaration: if, God forbid, the evidence reveals that Valve or its proxies have been conducting targeted cyberattacks against specific users to silence them, the international community will not play along. The rest of the world will not entertain your cute little legal games about exclusive jurisdiction in the courts of Washington State.

THE THREE DEMANDS — MINIMUM STANDARD OF FAIRNESS BEFORE ANY NEGOTIATION

1. **Answer the Crimea question publicly:** Does a court in annexed Crimea qualify as “any local Russian state court” under your ToS? Without a direct answer, no contact.

2. **Ban every account that used VPN to access Steam** — you have the database, you have the logs. You enforce this rule against theft victims. Apply it universally or admit it is selective.
3. **Return every asset stolen through trade substitution (API scam)** — start with every account ever listed on Lolzteam Market. You have the device identification logic. “Technically impossible” is not an answer.

We have no money to seize, no names to expose beyond what we have already published, and no corporate reputation to ruin. We are armed only with the truth and the patience to repeat it until it lands in a courtroom.

42. Final Verdict

`FINAL VERDICT — THREE DOCUMENTED FACTS FOR THE RECORD`

I. Steam killed the children it leaked. The data existed. The tools existed. The choice not to act was always a choice — not a limitation.

II. Steam steals from children under the guise of fighting “dupes” that were generated entirely by its own support staff. The Breakage Income is not a bug. It is a revenue line.

III. Steam lies about withholding ban reasons under the guise of “anti-cheat.” A Community Ban has nothing to do with VAC. The withholding is legally convenient, not technically necessary.

These statements are backed by eight years of documented evidence, official GDPR disclosures, LZT Market telemetry, and on-the-record legal communications. They are not allegations. They are conclusions of fact.

The bot is no longer under our management anyway. I feel no shame, and I do not believe I am doing a bad thing. I am certain we have no other choice. Source 1 stopped himself in time, but as far as we are concerned, you killed the children whose data you leaked to him. Therefore, we will not negotiate. Steam is the terrorist here.

Re-evaluate what you did, and what Source 1 was doing after your lawyers handed him that data. Where did your "Nikita" come from? And what about the four off-staff support agents sitting in Russia? I am sure you think this is an isolated incident, but we know about many of your cases and your "decisions."

We are not you. We do not cover up potential crimes. We will gradually release everything with proof and cooperate with any regulator — except the ones you seem to favor. Russian authorities write to us frequently; we usually tell them to fuck off, but maybe we will start answering. We don't play stupid games with unintelligible corporate responses designed to confuse, much like your user agreement.

I hope our position is absolutely clear:

Steam killed the children it leaked.

Steam steals from children under the guise of fighting "dupes" that were generated entirely by its own support staff.

Steam lies about withholding ban reasons under the guise of "anti-cheat" strictly because it is legally convenient. (What the fuck does anti-cheat have to do with a Community Ban?)

Are you really that confident your courts or Europe will just turn a blind eye? We will see.

References & Sources

[1] Netcraft Anti-Phishing Service and Reporter Prizes Program https://www.netcraft.com/anti-phishing/

[https://www.netcraft.com/anti-phishing/]

Netcraft is a leading internet security company that tracks and reports phishing sites. The Reporter Prizes program rewards verified submissions. Valve's refusal to cooperate with Netcraft is documented through public anti-phishing statistics.

[2] Cloudflare Abuse Reporting Portal https://www.cloudflare.com/abuse/ [https://www.cloudflare.com/abuse/]

Used for escalating phishing campaigns employing cloaking techniques against Cloudflare-protected infrastructure.

[3] Valve Internal Data Disclosure (2024) — Employee Count and Revenue Per Employee

Sources: Kotaku, Ars Technica, IGN, The Verge, PCGamer (May 2024)

https://kotaku.com/ [search: "Valve employees 2024"]

https://arstechnica.com/ [search: "Valve internal data leak"]

Internal documents revealed Valve's total headcount (~336) and the number of employees directly working on the Steam platform (~79), along with boasts about profit-per-employee exceeding Google, Amazon, and Microsoft.

[4] LZT Market (Lolzteam) — Shadow Marketplace Statistics https://lolz.live / https://lzt.market [https://lolz.live / https://lzt.market]

Russian-language clearnet marketplace for stolen accounts and cybercrime services. Item IDs (e.g., item_id 252853378) confirm cumulative listing history exceeding 250 million lots. Account counts cited reflect live marketplace data at time of documentation. Covered by: Group-IB, KELA Cyber Intelligence, and other threat intelligence providers.

[5] BlockBlasters Malware Incident on Steam (September 2024)

Security community reports and Steam community threads (September-October 2024):

https://www.reddit.com/r/GlobalOffensive/ [search: "BlockBlasters stealer"]

https://steamcommunity.com/

A game titled BlockBlasters was listed on Steam and distributed an information stealer. Reports submitted to Steam support beginning September 2, 2024 included open Telegram API endpoints embedded in game code. The game remained available for approximately one month before malicious builds were removed.

[6] Raivo Plavnieks — Content Creator and Whistleblower

Twitch streamer whose coverage of the BlockBlasters incident brought the malware to wider public attention. Documented through VODs, community posts, and security researcher reports (September 2024).

[7] ChainAbuse — Cryptocurrency Abuse Reporting Platform https://www.chainabuse.com [https://www.chainabuse.com]

Community-maintained database of cryptocurrency addresses associated with scams, ransomware, and fraud. Victims of the BlockBlasters stealer submitted reports to ChainAbuse documenting wallet addresses used to receive stolen cryptocurrency.

[8] IRS Form W-8BEN — Certificate of Foreign Status of Beneficial Owner https://www.irs.gov/forms-pubs/about-form-w-8ben [https://www.irs.gov/forms-pubs/about-form-w-8ben]

Required from non-US developers earning income through US entities (including Steam). This KYC document ties the developer's legal identity directly to their Steamworks publisher account, refuting Valve's "hacked anonymous developer" narrative.

[9] Taylor Wessing — International Law Firm https://www.taylorwessing.com [https://www.taylorwessing.com]

Offices in Hamburg, Munich, London, and other cities. Represents Valve Software in European legal matters including GDPR data subject access requests (DSARs). The firm's historical founding and its predecessor entities' documented connections to the Third Reich era have been the subject of academic and journalistic inquiry into German law firm histories.

[10] EU General Data Protection Regulation (GDPR) — Regulation 2016/679 https://eur-lex.europa.eu/eli/reg/2016/679/oj [https://eur-lex.europa.eu/eli/reg/2016/679/oj]

https://gdpr.eu/

Under Article 15 GDPR, data subjects may request full disclosure of personal data held. Valve's compliance with DSARs has been processed through Taylor Wessing, and documented cases show improperly redacted responses disclosing data of third parties — including minors.

[11] RedLine Infostealer — Operation Magnus (October 28, 2024)

Europol Press Release: https://www.europol.europa.eu/media-press/newsroom/news/operation-magnus-redline-and-meta-infostealers-dismantled

FBI and Dutch National Police (Politie) participated in the takedown of RedLine and META stealer infrastructure. RedLine was the dominant tool for stealing Steam session files (SSFN) and browser cookies during 2021-2024, sold as Malware-as-a-Service (MaaS) on Russian-language forums.

Additional coverage: BleepingComputer (October 2024), The Record, Krebs on Security.

[12] SteamRep — Community Trading Reputation Database https://steamrep.com [https://steamrep.com]

Volunteer-run platform that tracked scammers in Steam trading communities. Internal controversies, including alleged bribery for scammer tag removal and administrative corruption, were documented in community forum threads circa 2016-2020. Valve severed formal cooperation with SteamRep-affiliated moderators by 2022.

[13] Jess Cliffe — Counter-Strike Co-Creator

Reported by: Kotaku, Polygon, PC Gamer, The Verge (September 7-8, 2016)

https://kotaku.com/ [search: "Jess Cliffe Valve"]

Valve placed Jess Cliffe (credited alongside Minh Le for creating Counter-Strike) on administrative leave in 2016 following his arrest on charges of commercial sexual abuse of a minor. He was subsequently terminated without a court conviction.

[14] Valve Steam Trade Hold Policy

Steam Blog announcement on trade holds (December 9, 2015):

https://steamcommunity.com/games/593110/announcements/detail/

The 7-day hold on traded items was formally introduced in December 2015. Earlier escrow mechanisms were introduced starting 2012. The policy change was intended to reduce fraud but in practice created the linear theft pipeline described in this report.

[15] Valve Anti-Cheat (VAC) System

Official documentation: https://support.steampowered.com/kb_article.php?ref=7849-Radz-6869

VAC bans are account-wide, permanent, and tied to the hardware/phone number used during the violation. The asymmetric application of VAC bans (aggressive for cheating, absent for mass phishing activity) is documented through community tracking at vacbanned.com and similar resources.

[16] FBI Seattle Field Office

Address: 1110 3rd Ave, Seattle, WA 98101

Phone: +1 (206) 622-0460

https://www.fbi.gov/contact-us/field-offices/seattle

Valve Software is headquartered at 10400 NE 4th St, Bellevue, WA 98004 — within the FBI Seattle field office jurisdiction.

[17] IC3 — Internet Crime Complaint Center (FBI) https://www.ic3.gov [https://www.ic3.gov]

The FBI's official portal for reporting cybercrime, including account theft, fraud, and sanctions violations. Accepts reports from individuals, businesses, and third parties.

[18] CISA — Cybersecurity and Infrastructure Security Agency https://www.cisa.gov [https://www.cisa.gov]

US federal agency responsible for critical infrastructure cybersecurity. CISA's Stop Ransomware and Known Exploited Vulnerabilities programs are relevant to the infostealer ecosystem documented here.

[19] DOJ NSD — Department of Justice, National Security Division https://www.justice.gov/nsd [https://www.justice.gov/nsd]

Oversees national security cases including sanctions violations (OFAC referrals), foreign influence operations, and cyber threats tied to nation-state actors. The potential nexus between state-adjacent structures controlling LZT Market and Steam's platform policy warrants NSD attention.

[20] OFAC — Office of Foreign Assets Control (U.S. Treasury) https://ofac.treasury.gov [https://ofac.treasury.gov]

Russia-related sanctions programs: https://ofac.treasury.gov/sanctions-programs-and-country-information/russia-related-sanctions

Ukraine-EO13685 (Crimea), and subsequent executive orders cover the DNR/LNR regions. Accepting payments originating from sanctioned persons or territories — whether directly or through intermediaries — may constitute sanctions violations subject to civil and criminal penalties.

[21] JSON Web Token (JWT) — RFC 7519
https://datatracker.ietf.org/doc/html/rfc7519
[https://datatracker.ietf.org/doc/html/rfc7519]

Industry-standard method for representing claims between parties. Steam adopted JWT-based session tokens as a replacement for legacy SSFN files. The off-platform validation capability of JWTs (verifiable without querying Steam servers) is a documented property of the specification.

[22] Steam Direct — Developer Application and KYC
https://partner.steamgames.com/steamdirect
[https://partner.steamgames.com/steamdirect]

Valve charges $100 per game submission and requires developers to submit legal identification, tax forms (W-8BEN for non-US), and banking information. This KYC process creates a paper trail that directly contradicts the "anonymous hacker" narrative.

[23] Roskomnadzor — Federal Service for Supervision of Communications, Information Technology and Mass Media (Russia) https://rkn.gov.ru [https://rkn.gov.ru]

The Russian federal regulator has issued multiple administrative decisions against LZT Market (Lolzteam) ordering its blocking. These decisions have been publicly available in Russian regulatory databases. The market's continued operation despite five such decisions points to legal maneuvering and possible political protection.

[24] FunPay — Russian Peer-to-Peer Trading Platform
https://funpay.com [https://funpay.com]

Widely used platform in CIS regions for trading in-game goods, including Steam balance top-ups and region-switching services. Transaction counts cited (500,000+) reflect documented seller statistics visible on the platform's seller profiles.

[25] Tinkoff Bank — Sanctioned Russian Financial Institution

Tinkoff Bank (now T-Bank) was added to OFAC SDN list and subjected to EU sanctions following Russia's 2022 invasion of Ukraine.

OFAC SDN list: https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

Steam accounts were documented receiving top-ups from Tinkoff-issued cards in the CIS region after the imposition of sanctions.

[26] Uniswap Protocol — Decentralized Exchange
https://uniswap.org [https://uniswap.org]

Uniswap and broader DeFi protocols have been targeted by phishing operations whose techniques and personnel originated in the Steam scam ecosystem. Security reports from Chainalysis, CertiK, and SlowMist document the migration of CIS-region fraudsters from gaming scams to Web3 drainer attacks.

[27] Steam Session Files (SSFN) — Technical Documentation

Community and security researcher documentation:

https://steamdb.info / https://github.com/nicklvsa (various Steam security research repos)

SSFN (SteamSentryFile) files stored Steam Guard authentication tokens locally. When stolen by infostealers, they allowed session reuse without re-authentication. Valve deprecated SSFN in favor of JWT-based sessions during 2023-2024.

[28] Binance / Bybit / Gate.io — Cryptocurrency Exchanges https://www.binance.com | https://www.bybit.com | https://www.gate.io
[https://www.binance.com | https://www.bybit.com | https://www.gate.io]

Major centralized exchanges whose Telegram payment bots and P2P trading infrastructure are used by LZT Market and similar platforms to process payments for stolen account transactions, circumventing traditional AML controls.

[29] Steam Phishing via Google Ads — Documented Campaigns (2023-2024)

Reported by: BleepingComputer, Malwarebytes, Group-IB

https://www.bleepingcomputer.com/ [search: "Steam phishing Google Ads"]

https://www.malwarebytes.com/ [search: "Steam phishing ads"]

Attackers purchased Google Ads targeting Steam-related search queries, substituting display URLs to appear as legitimate Steam domains. The scale of the 2024 campaign documented by PhishDestroy ($300,000 estimated net proceeds) aligns with Google Ads abuse patterns documented by multiple cybersecurity firms.

[30] STALKER 2 / GTA — Games Whose Publishers Withdrew from Russian Market

GSC Game World (STALKER 2) officially suspended sales in Russia following the 2022 invasion of Ukraine.

Rockstar Games / Take-Two Interactive restricted GTA sales in Russia following sanctions.

Despite publisher intent, Steam continued to provide mechanisms allowing Russian users to purchase these titles via region-switching, as documented by community researchers and gaming press (Eurogamer, RPS, IGN, 2022-2024).

ADDITIONAL CONTEXT: REGULATORY AND LEGAL FRAMEWORK

Steam's Terms of Service (ToS), Version History:

The Steam Subscriber Agreement is archived by the Internet Archive Wayback Machine:

https://web.archive.org/web/*/https://store.steampowered.com/subscriber_agreement/

Comparison of versions shows modification of sanctions-related language, including the removal of explicitly named countries (Cuba, Iran, Syria) from prohibited territory lists.

AML / FATF Guidelines on Virtual Assets:

Financial Action Task Force (FATF) guidance on virtual assets and virtual asset service providers:

https://www.fatf-gafi.org/en/topics/virtual-assets.html

Skin trading platforms and Steam Wallet function as virtual asset ecosystems subject to FATF Recommendation 15.

Europol — Internet Organised Crime Threat Assessment (IOCTA):

https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Annual reports document the role of gaming platforms in cybercrime recruitment and infostealer distribution.

Group-IB — Hi-Tech Crime Trends Report:

https://www.group-ib.com/resources/research/

Documents the evolution of CIS-region cybercrime from gaming-platform fraud to ransomware and financial crime.

Chainalysis Crypto Crime Report:

https://www.chainalysis.com/blog/crypto-crime-report/

Annual report documenting laundering of cybercrime proceeds through decentralized exchanges and peer-to-peer platforms, including those accepting Steam-ecosystem stolen goods.

NOTE ON SOURCES

All market statistics cited (LZT Market account counts, transaction volumes, JWT token prices) reflect data documented at specific points in time by PhishDestroy through direct platform observation. Shadow market data is inherently dynamic; figures cited represent point-in-time measurements and directional trends, not static permanent values. Where possible, archived copies of relevant pages have been preserved on the Wayback Machine (web.archive.org) and independent archival nodes.

All regulatory contact information (FBI, IC3, CISA, DOJ NSD, OFAC) reflects publicly available official contact data as of the date of this publication.

PHISHDESTROY DEMANDS

Valve must be held financially accountable for accounts stolen through their deliberate negligence. The minimum estimated liability: **$450,000,000** — representing the documented victim real spend on accounts currently listed on LZT Market across all categories, and the value of inventories frozen on banned bots that were never returned to victims.

> This is not an estimate of criminal market value. This is the documented money victims spent on their accounts — money that Steam's negligence, outsourced corruption, and deliberate API blindness allowed to be stolen and re-monetized on criminal markets while Valve collected commission on both the original sale and every subsequent stolen skin transaction.
>
> Valve wrote the policy that prevents item restoration. Valve's outsource staff committed the thefts. Valve's API enabled the marketplace. Valve's 15% commission runs on the same skins. The accountability is structural, not incidental.

Inside the report

← Related: Steam Shadow Economy (Part I) [/steam-shadow-economy]