TLP:CLEAR CTI-LATAM-2026-001 · PUBLIC EDITION V2 · UNRESTRICTED DISTRIBUTION

FIELD INVESTIGATION · CASHCLOAK LATAM · CTI-LATAM-2026-001

Verified ads, destinations that do not match

How fake investments and card forms reach Argentine users. Over two days of normal phone use I saw paid ads, marked “Sponsored” and with the advertiser identity verified by Google, that led to fake news articles, investment chatbots, card forms carrying the brand of an Argentine broker and phone-number capture for a call center. The pieces share an audience, brands and persuasion techniques, but not a proven owner.

REPORT ID
CTI-LATAM-2026-001 · v2

AUTHOR
Ezequiel Jorge La Terra
ORCID 0009-0008-1677-4218

OBSERVATION
30 Sep and 1 Oct 2026
(Argentina time)

PUBLICATION
October 2026

CLASSIFICATION · LICENSE
TLP:CLEAR · CC BY 4.0

CONTENTS

01 Executive summary
02 Key findings
03 What it is and what it is not
04 What a verified ad proves
05 The path
06 The verticals
07 What they share
08 Proven and not proven
09 Impact
10 Indicators (IOCs)
11 MITRE ATT&CK
12 Recommendations
13 Method and limitations
14 Conclusion
15 Coordinated disclosure
16 How to cite and license

01 · EXECUTIVE SUMMARY

It is not a gang: it is a traffic market

Between 30 September and 1 October 2026 (Argentina time) I observed, as an ordinary user, paid ads aimed at Argentine users, many of them with the advertiser identity verified by Google, that led to fake news articles with an investment chat, chatbots posing as a Mercado Libre “personal manager” and a “Mercado Pago CFD” path that ends in lead capture for a call center. On the same days I also documented a card form asking for the security code that uses the Balanz brand without being Balanz.

The declared advertisers are in at least six countries (United Kingdom, Cyprus, the Netherlands, Ukraine, Australia and Brazil), and I could not establish a common operator. The evidence describes a **traffic-acquisition circuit**: traffic buyers and templates working on the same audience, not one person or one group. For defenders, this means that blocking domains helps but comes late: the earliest point of intervention is the ad, and the most concrete one for a bank is the customer’s first transaction towards a “broker” nobody knows.

CASHCLOAK LATAM is the tracking name I use at Cyber Threat Intelligence LATAM for this investigation. It is a working label, not the name of a group or an actor.

02 · KEY FINDINGS

Seven findings

01 **The entry point is paid, verified advertising.**
Google ads in the browser and in Gmail Promotions with the label “Advertiser identity verified by Google”. That verification confirms who pays for the ad, not that the offer is legitimate.

02 **The declared advertisers are many and dispersed.**
Advertisers declared in at least six countries (United Kingdom, Cyprus, the Netherlands, Ukraine, Australia and Brazil), with ads aimed at Argentine users. This is consistent with a market of traffic buyers, not with a single operator.

03 **The ad’s domain and the destination’s domain may not match.**
An ad that showed a women’s fashion site led to a fake investment article on another domain. This is compatible with a redirect or with cloaking; from the user’s side it is not possible to determine which of the two happened.

04 **Mercado Libre is the brand most used as a lure,**
in at least three formats: a fake article with chat, a “personal manager” chatbot and “Mercado Pago CFD”. Sharing a brand does not show that they share an operator.

05 **A site with the Balanz brand asks for the full card, including the security code.**
It is not Balanz. Asking for the CVC in its own form in order to “deposit” is a serious risk signal, although it could not be confirmed that cards were stolen.

06 **Not everything that appears in this circuit is fraud.**
An “ANSES Loans Guide” landing page showed thematic content without asking for sensitive data. It is included as context, not as phishing.

07 **A verified ad pointed to a generic subdomain**
that does not refer to any known brand. It is published as a hunting indicator, without claiming what content it served.

▲ 03 · SCOPE

▲ What this publication is and what it is not

Everything I describe I saw as any user would: the ads shown on a phone, the information Google provides in “My Ad Center” when tapping the three dots on each ad, and the pages that opened when tapping the ad. I keep the screenshots with their cryptographic hash so that every claim can be audited.

This edition does **not** attribute anything to individuals, does **not** claim that the declared advertisers operate the destination sites and does **not** hold that all destinations belong to the same operation. Nor does it claim that Google, Mercado Libre, Balanz, YPF, La Nación, ANSES or the banks whose logos appear took part: they are platforms or brands used as lures.

ROLES BEFORE NAMES

ROLE	WHAT IT DOES	WHAT IT DOES NOT IMPLY
Declared advertiser	Appears as the payer of the ad in “My Ad Center”, with country and verified identity	It does not imply that it designs the fraud, controls the destination or knows what content is served
Displayed domain	The site that appears in the ad	It may be a front site, different from the real destination
Destination or landing page	The page that actually opens	It may rotate, change content or belong to a third party
Conversion step	Chat, phone form, card form	The type of step defines the harm: a lead is not the same as a CVC
Impersonated brand	Mercado Libre, Balanz, La Nación, YPF, banks, ANSES	**It is a victim, not a party**
Advertising platform	Serves the ad and publishes the disclosure	Its verification covers the payer’s identity, not the offer

> I do not name or identify in any way the advertisers listed as payers, nor do I indicate what type they are; their data goes only to the platform, through the corresponding reporting channel. I refer only to their declared country, because what matters is the pattern and not who is listed as the account holder.

▲ 04 · THE TRUST SIGNAL

▲ What a “verified” ad proves and what it does not

“My Ad Center” is one of the most useful transparency tools available to a user: by tapping a Google ad you can see who paid for it, its declared location and whether its identity was verified. Every relevant ad I observed carried the label “Advertiser identity verified by Google”.

That information proves that there is an advertising account whose declared holder passed identity verification and paid for that ad. **It does not prove** that this holder designed the destination content, collects the money or runs the scam: it may be an affiliate paid per click or per lead, an intermediary, or someone whose business identity was used by another party. That is why I treat the disclosure as a starting point for the platform, not as an attribution.

> **The underlying problem:** the verification signal describes the payer, but users read it as if it described the offer. A “verified” ad that leads to an article with the design of a national newspaper is perceived as doubly trustworthy.

05 · THE PATH

From attention to data

The observed verticals do not all go through the same steps, but they fit a common scheme:

1 →

Paid ad

“Sponsored”, with verified advertiser identity.

2 →

Displayed domain → real destination

SOMETIMES DIFFERENT

The site in the ad may not be the page that opens.

3 →

Persuasion

Fake article, well-known brand, borrowed authority, urgency.

4 →

Conversion

Chat · phone (+54) · full card with CVC.

5

Next step outside the page

Call, “bond”, “deposit”.

> The arrows describe a user’s path, not a relationship between operators. That two destinations share a step does not mean they are run by the same person.

06 · AD PATHS

Six verticals and a generic destination

Seen one by one, they look like isolated scams. What can be observed is that almost all of them arrived the same way: paid advertising, shown as “Sponsored” in the browser, in Gmail’s Promotions tab or on native ad networks. Some destinations ask for card data; others, a phone number; others only show content. Not all of them are fraud, and this is made clear in each case.

VERTICAL 1

BLOCK

The fake news article with an investment chat

A Google ad showed a women's fashion site; its disclosure identified as payer an advertiser declared in Ukraine. Tapping it opened `lunarbutton[.]site`, with an article imitating the design of La Nación: an investment platform "linked to Mercado Libre" and "backed by public figures" promised 450% on a minimum of 200,000 pesos. Then came a WhatsApp-style chat, logos of banks operating in Argentina and the key word of advance-fee fraud: a "bond" to be paid before collecting.

Another ad, with a payer declared in Australia, led to a fake article with the same design that used the names of public figures. The change of domain is compatible with a redirect or with cloaking; I do not claim either.

Why it matters. An ad review that looks at the displayed domain (a clothing site) and not at the final destination misses exactly the step where the fraud is.

VERTICAL 2

BLOCK

The Mercado Libre "personal manager"

`epicharvest[.]info` arrived through a Google ad with a payer declared in the Netherlands and a verified identity. It was a chatbot posing as a Mercado Libre "personal manager", with plans of 5, 10 and 20 million pesos, "verified by YPF", that promised to turn 150,000 pesos into 5,000,000 a month. It ended in a form with the +54 prefix and a "Thank you!" page.

I assess with **moderate confidence** that it shares a chat template with vertical 1. That is not enough to say they are run by the same person: these templates are sold and copied.

Why it matters. The product is not an immediate payment but a contact: an Argentine phone number willing to hear an investment offer.

VERTICAL 3

NO PUBLIC IOC

Lead-capture forms with “leverage”

In Gmail Promotions, a Mercado Libre banner offered trading with “200:1 leverage” (advertiser declared in the United Kingdom). Another ad (advertiser declared in Cyprus) led to an identical form: same design, a minimum deposit of 100 dollars and the same e-wallets. I assess with **moderate confidence** that it is the same template used by two payers, a typical pattern of high-risk investment affiliate networks.

I do not claim that these pages are fraudulent; that is why their domains are not published as indicators and are kept for the report to the platform.

VERTICAL 4

BLOCK

A card requested in order to “deposit”

`app.balanztrading[.]com` uses the brand of Balanz, a real Argentine financial firm, with a “deposit” form that asks for card number, holder, expiry date and security code, alongside “PCI-DSS compliant” and 3-D Secure seals. **It is not Balanz**: the impersonated brand is a victim. The screenshots do not record which ad led to this page, so it is not associated with any advertiser.

Asking for the CVC in its own form, outside a recognizable payment processor, is a serious risk signal. It could not be confirmed that cards were stolen or that charges were made.

Why it matters. For a bank, a card entered on a site like this is a potentially compromised card before the first suspicious charge.

VERTICAL 5

HUNT

“Mercado Pago CFD” and the call center

On native ad networks (the “recommended content” blocks at the bottom of news sites), three different advertisers offered “Mercado Pago/Mercado Libre CFDs”. The path: a landing page imitating a “payments app” that asked for a +54 phone number; then `falcon-press[.]com`, with the notice that “an investment executive will call you”; and finally `lpa.voltfalcon-press[.]com`, with a sub-affiliate identifier that is not published.

I assess with **moderate confidence** that this is lead capture for an investment call center: the pressure and the request for money happen later, by phone.

Why it matters. When the conversion is a phone number, blocking the domain comes late. The useful defense is earlier (at the ad) and later (in the bank’s alert on the first transfer to a “broker”).

VERTICAL 6

NO PUBLIC IOC

ANSES as a commercial hook, with no phishing observed

ANSES-themed advertising in Gmail Promotions led to an “ANSES Loans Guide” landing page on an Argentine subdomain of a Brazilian site (advertiser declared in Brazil). The domain is not published as an indicator. No sensitive-data form or payment request was observed. **It is not classified as phishing.** It is included as context because using a social security agency as a hook confuses an especially exposed audience.

GENERIC DESTINATION

HUNT

An unbranded subdomain, paid and verified

A “Sponsored” ad, from an advertiser declared in Brazil with a verified identity, led to `descubre.upmegaconectnotification[.]click`. There is no screenshot of the content, so it is not described and no vertical is assigned to it. It is published for **hunting, not blocking**, because of three traits: a paid and verified destination, a generic unbranded name and a low-cost extension frequent in disposable infrastructure.

▲ 07 · PATTERN

▲ What they share: a repertoire, not a server

- **Borrowed authority.** A national newspaper, a state-owned oil company, banks, a broker, a public agency, the largest marketplace in the region.
- **Verification as a shield.** The “verified” ad transfers its credibility to the destination, even though it only covers the payer.
- **Disproportionate promises.** 450%, 150,000 pesos turned into 5,000,000 a month, 200:1 leverage.
- **An upfront charge.** “Bond”, “minimum deposit”, “deposit by card”.
- **A conversion that leaves the page.** Chat, call, form: the harm is completed in a channel the page does not show.

That repertoire is compatible with a market of templates, affiliates and traffic buyers. A common operator could not be established, and the diversity of payers and countries suggests the opposite: many actors competing for the same victims with the same tools.

▲ 08 · LEVEL OF CERTAINTY

▲ What is proven and what is not

CLAIM	STATUS
There were paid ads aimed at Argentine users with the advertiser identity verified by Google	OBSERVED
Those ads led to fake articles, investment chatbots, phone-number capture and a card form with CVC	OBSERVED
At least one ad showed one domain and led to another	OBSERVED
That jump is due to cloaking	NOT DETERMINED Compatible with a redirect or cloaking
Two chatbots use the same template	ASSESSMENT · MODERATE
Two lead-capture forms use the same template	ASSESSMENT · MODERATE
The “Mercado Pago CFD” path feeds a call center	ASSESSMENT · MODERATE
The declared advertisers operate the destinations	NOT ESTABLISHED
All verticals belong to the same operation or actor	NOT ESTABLISHED
Cards were stolen or charges were made	NOT CONFIRMED
The ANSES landing page is phishing	NO No capture of sensitive data was observed
Google, the brands or the banks take part	NO They are a platform or impersonated brands

▲ 09 · IMPACT

▲ Who it hits and where

Users. The fraud arrives with every sign of legitimacy they were taught to look for: a well-known search engine, the verification label, the design of a national newspaper, their bank’s logo. “Be wary of odd sites” is not enough when the odd site arrives wrapped in official signals.

Impersonated brands. Reputational and support damage: defrauded users complain to Mercado Libre, to Balanz or to their bank, not to the advertiser.

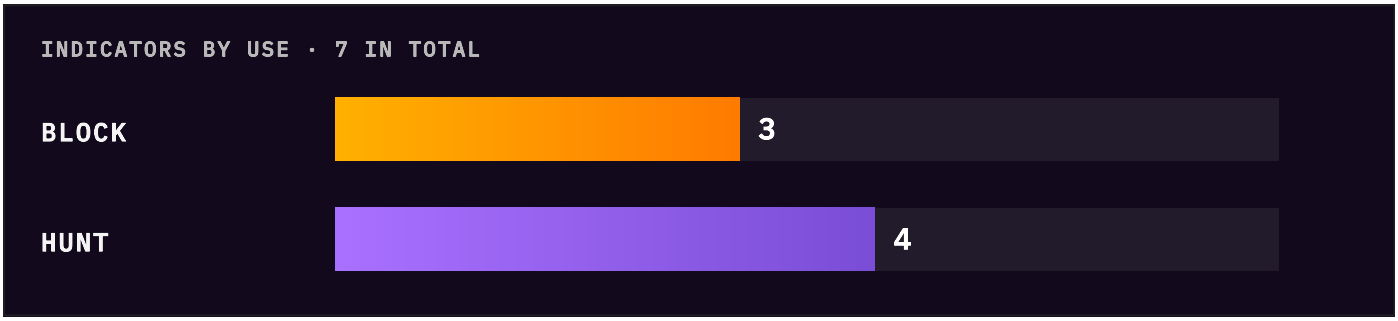
Banks and fintechs. The risk materializes in the card entered in a “deposit” form and in the transfers that follow the call from an “investment executive”. In both cases the first sign reaches the bank before any blocklist.

Advertising platforms. The case shows the limit of verifying only the payer’s identity when the destination can change or not match the displayed domain.

▲ 10 · INDICATORS

▲ Indicators of compromise (IOCs)

Seven domains, all **defanged** (`[.]`): **do not visit them**. To import them, replace `[.]` with `.` . `first_seen` is the date of my first observation (Argentina time), not the domain’s creation date.



CASHCLOAK_IOCS_PUBLIC_EN.CSV · 7 INDICATORS (3 BLOCK · 4 HUNT) · TLP:CLEAR

INDICATOR	USE	SEEN	NOTE
`lunarbutton[.]site`	BLOCK	2026-10-01	Fake article with La Nación's design and an investment chat with Mercado Libre branding (minimum ARS 200,000, 450%, "bond"). Reached from a Google ad that showed another domain.
`epicharvest[.]info`	BLOCK	2026-09-30	Fake Mercado Libre "personal manager" chatbot ("verified by YPF"), +54 form. Block only the FQDN. Link to the other indicators: not established.
`app.balanztrading[.]com`	BLOCK	2026-09-30	"Deposit" form with the Balanz brand asking for the full card, holder, expiry date and CVC. **It is not Balanz.** Block only the FQDN; the parent domain is not published as an indicator.
`descubre.upmegaconectnotification[.]click`	HUNT	2026-09-30	Destination of a Google ad with verified advertiser identity. Content not documented. Log hunting only.
`upmegaconectnotification[.]click`	HUNT	2026-09-30	Parent domain of the previous one. Hunting only; do not block (low public specificity).
`falcon-press[.]com`	HUNT	2026-10-01	Step in a "Mercado Pago CFD" path from native ads ("an investment executive will call you"). Assessed as lead capture for a call center. Hunting only. No claim is made about who holds the domain.
`lpa.voltfalcon-press[.]com`	HUNT	2026-10-01	Final step of the same path, with a sub-affiliate identifier (not published). Hunting only. No claim is made about who holds the domain.

- BLOCK destinations with observed fraudulent content. They can be blocked by FQDN.
- HUNT search DNS and proxy logs; do not block without your own analysis.

▲ 11 · TECHNIQUES

▲ Mapping to MITRE ATT&CK

ATT&CK is used only where it represents what was observed well.

TECHNIQUE	WHAT WAS OBSERVED
T1583.008 · Acquire Infrastructure: Malvertising	Paid ads leading to fake-investment destinations
T1656 · Impersonation	Use of the Mercado Libre, Balanz, La Nación, YPF and bank brands
T1056.003 · Input Capture: Web Portal Capture	Card form with CVC (data capture not confirmed)

As a complement, the MITRE Fight Fraud Framework (F3) is better suited than ATT&CK Enterprise to describe financial fraud against consumers.

▲ 12 · RECOMMENDATIONS

▲ What to do, by role

USERS

- Before entering data, check the real address of the page, not the one in the ad.
- Be wary of any guaranteed return and of any “bond” to release earnings.
- No legitimate broker asks for your card’s security code in its own form in order to “deposit”.
- “Verified identity” refers to who pays for the ad, not to the offer.
- If an ad looks misleading, report it from the ad itself.

BANKS, FINTECHS AND BRANDS

Banks and fintechs

Treat as a risk signal the first transfers or card payments to unknown CFD “brokers” or investment platforms, especially from customers with no investment history. Warn in customer communications that no legitimate party asks for the CVC in order to “deposit”, or for a “bond”.

Fraud prevention

Search for the indicators in proxy and DNS logs and cross-check those visits with later transactions. Watch for the script’s words in complaints: “bond”, “personal manager”, “verified by YPF”, “an executive will call you”.

Impersonated brands

Monitor the use of their name in paid ads with the public ad-transparency tools, and publish clear official channels about what they never ask for.

PLATFORMS AND COMMUNITY

Advertising platforms

Review the final destination and not only the displayed domain, and treat a mismatch between the two as a signal. Tell users that verification covers the payer, not the offer.

SOC and CTI

Block the BLOCK indicators; hunt for the HUNT indicators without blocking. Analyze the destinations with a profile similar to the victim’s (phone, local connection, arrival from an ad): from another context a different page may be shown.

CERTs and CSIRTs

Receive the indicators and, where appropriate, coordinate with the brands and with the registrars of the domains marked for blocking.

13 · METHOD AND LIMITATIONS

How it was done and how far it goes

METHOD

- **Passive observation, as a user.** Ads shown on a phone during two days of normal use (30 Sep and 1 Oct 2026, Argentina time), in the browser, in Gmail Promotions and on native ad networks.
- **Payer source.** The public information in Google’s “My Ad Center” for each ad: declared payer, location and verification status.

- **Destinations.** Only the pages that opened when tapping the ad, documented with screenshots kept with their cryptographic hash.
- **Language of certainty.** Each claim is marked as observed, assessed (with a confidence level) or not established.

LIMITATIONS

- It is a small sample: one phone, two days. **It does not measure prevalence** or reach.
- From the user's side it is not possible to distinguish a redirect from cloaking, or to know what another visitor or the platform's reviewer sees.
- There is no screenshot of the generic destination's content, and it was not recorded which ad led to the form with the Balanz brand.
- No technical relationships between destinations were established; the template matches are moderate-confidence assessments.
- It is not known who operates the destinations, whether any of them shares an owner with another, or how many people entered their data.
- The destinations may rotate or change content after the observation.

14 · CONCLUSION

The entry point, not the infrastructure

These scams do not resemble each other in their infrastructure but in their entry point. Each vertical on its own is known: the fake article, the investment chatbot, the broker that asks for the card. What changes the reading is seeing them together, on the same days, arriving through paid and verified ads, with payers in at least six countries (United Kingdom, Cyprus, the Netherlands, Ukraine, Australia and Brazil) and the same list of Argentine brands as lures.

The threat is not a gang but a market: advertisers who buy traffic, templates that are reused and destinations that turn attention into a phone number, a deposit or a card. Blocking domains helps, but it comes afterwards. **I did not connect what the evidence does not connect.**

15 · COORDINATED DISCLOSURE

Coordinated disclosure

> Before publication, the findings were reported to incident response teams in the region and to the impersonated brands.

How to cite

> La Terra, Ezequiel Jorge (2026). *CASHCLOAK LATAM: verified ads and investment- and card-fraud destinations aimed at Argentine users* (CTI-LATAM-2026-001, public edition v2). Cyber Threat Intelligence LATAM. https://cyberthreatintelligence.lat/en/report/cashcloak-latam/

```
@techreport{laterra2026cashcloak,
  author      = {La Terra, Ezequiel Jorge},
  title       = {{CASHCLOAK LATAM}: verified ads and investment- and card-fraud
                 destinations aimed at Argentine users},
  institution = {Cyber Threat Intelligence LATAM},
  number      = {CTI-LATAM-2026-001},
  year        = {2026},
  note        = {Public edition v2, TLP:CLEAR},
  url         = {https://cyberthreatintelligence.lat/en/report/cashcloak-latam/},
}
```


LICENSE

Text and data under Creative Commons Attribution 4.0 International (CC BY 4.0). They may be reused and adapted, including for commercial purposes, with attribution.

NOTICE

> This publication describes observations made as a user and analytical assessments marked as such. It does not attribute responsibility to individuals or companies. The declared advertisers are mentioned only by their country and are not presumed responsible for the destinations. The brands and platforms named are victims of impersonation or providers of a service, not parties. Corrections are published, with their date, in the corrections log.

© 2026 Ezequiel Jorge La Terra · Cyber Threat Intelligence LATAM · TLP:CLEAR · CC BY 4.0