# Network Takedown Confirmed — Six Apps, Two Developer Accounts, One Operator

## Spinwinera app, Spinwinera, Spinwinera Casino, Roobet, BetOnRed

Two Play developer accounts, one casino brand family, six listings, a seven-domain constellation, EU funnels in six member states. All now confirmed gone.

**RESOLVED • ENTIRE IDENTIFIED NETWORK CONFIRMED REMOVED FROM THE GOOGLE PLAY STORE**

| | |
|---|---|
| **Analyst** | RFI-IRFOS Research Team |
| **Filed** | 2026-07-01 (three coordinated reports: SPINWINERA-001, -A, -B) |
| **Confirmed** | 2026-07-07 (SPINWINERA-001 05:18 UTC, SPINWINERA-B 05:34 UTC) |
| **Account 1** | HOME ESSENTIALS & HARDWARE LIMITED, London W9 3EF, UK |
| **Account 1 apps** | Merge Chicken, Spinwinera app, Spinwinera |
| **Account 2** | ASJ ALL IN ONE SERVICES LIMITED |
| **Account 2 apps** | Spinwinera Casino, Roobet, BetOnRed |
| **Shared brand / C2** | spinwinera.com + 6 domain variants |
| **EU affiliate funnels** | BE / DE / LU / ES / IT / CH |
| **Related case** | MERGECHICKEN-001 (removed 2026-06-30) |
| **Severity** | CRITICAL |
| **Time to outcome** | 6 days (SPINWINERA-001/B); 5 days (MERGECHICKEN-001) |

## Contents

## Executive Summary

On 2026-06-30, Google Play & Android Security confirmed removal of ”Merge Chicken” (com.Merge.o98Chickens): a PEGI 3 listing concealing an unlicensed real-money casino, delivered at runtime via Firebase Remote Config from spinwinera.com. RFI-IRFOS’s report on that case closed with a residual-risk warning: the developer account also operated ”Spinwinera”, and package-level takedowns do not remove an actor’s capacity to re-list.

That warning proved conservative. Follow-on investigation, conducted the same day Google invited further leads, found not one but two Play developer accounts distributing the same casino brand family: HOME ESSENTIALS & HARDWARE LIMITED (Merge Chicken, plus two further listings named directly after the casino — ”Spinwinera app” and ”Spinwinera”) and a sibling account, ASJ ALL IN ONE SERVICES LIMITED (”Spinwinera Casino”, ”Roobet”, ”BetOnRed”). Three coordinated reports were filed the same day: SPINWINERA-001 (fresh lead, account-level ask), SPINWINERA-A (independent binary analysis of the still-live com.win.era.appofficial), and SPINWINERA-B (cross-account operator attribution, tracing the brand back to a prior, previously-unattributed April 2026 enforcement action).

On 2026-07-07, Google confirmed two of the three filings within the same sixteen minutes: ”We can now confirm that the apps are no longer available on the Play Store” (SPINWINERA-001, 05:18 UTC) and, separately, the identical confirmation on SPINWINERA-B (05:34 UTC) covering the ASJ ALL IN ONE SERVICES LIMITED account. Between the two accounts, six app listings built around one casino brand are now off the Play Store.

What this case adds beyond MERGECHICKEN-001 is scale and structure: two incorporated fronts rather than one, a seven-domain hosting constellation, EU affiliate/CPA funnels observed across six member states, and a demonstrable pattern of re-incorporation after enforcement (the ASJ account’s three listings were already removed once, in April 2026, before this investigation connected them to the same operator). This is accordingly treated below not only as an app-security matter but as a cross-border financial-crime, consumer-protection and corporate-structuring matter, and the report is organised across those disciplines. One artifact remains live and out of Play Store scope: the storefront cover website app.homeessentials.shop, addressed under Residual Risk.

**Scope:** This report spans three coordinated filings with different evidentiary bases, stated plainly: MERGECHICKEN-001 (com.Merge.o98Chickens) was fully binary-confirmed — hardcoded Firebase Remote Config payload to spinwinera.com. SPINWINERA-A (com.win.era.appofficial) was independently decompiled (apktool, string/resource analysis over classes.dex, libil2cpp.so and IL2CPP global-metadata.dat); it carries no hardcoded casino URL, but a bespoke anti-emulator/anti-sandbox detection signature was recovered from the binary — a legitimate cleaning-game has no reason to fingerprint BlueStacks or Houdini ARM-translation. SPINWINERA-001 (com.spinwinera.app) and SPINWINERA-B (the three ASJ-account listings, already removed by Google as of April 2026 before this report was filed) rest on actor-level and brand-level linkage rather than fresh decompilation of those specific binaries, disclosed to Google explicitly as such. The corporate, financial-crime and cross-border analysis below is desk research over open-source company-registry and domain-registration data; it is analysis for the competent authorities, not a legal determination.

**Disposition**

Three reports filed 2026-07-01, the day Google invited further leads following the Merge Chicken takedown. All three acknowledged within hours. On 2026-07-07: SPINWINERA-001 confirmed at 05:18 UTC ("We can now confirm that the apps are no longer available on the Play Store"); SPINWINERA-B confirmed at 05:34 UTC, same wording, covering the ASJ ALL IN ONE SERVICES LIMITED account. SPINWINERA-A's target package (com.win.era.appofficial) is the same package confirmed under SPINWINERA-001. Third and fourth confirmed enforcement outcomes of the RFI-IRFOS 2026 Android audit programme, all against a single underlying operator.

| ID | Severity | Title |
|---|---|---|
| SW-01 | CRITICAL | Two-account operator network built on one casino brand |
| SW-02 | CRITICAL | Bespoke anti-emulator / anti-sandbox detection in a children's cleaning game |
| SW-03 | CRITICAL | Live, unlicensed real-money casino and sportsbook at the shared domain |
| SW-04 | HIGH | Age-rating contradiction across the network |
| SW-05 | HIGH | Corporate identity inconsistency - UK-registered front, US contact number |
| SW-06 | HIGH | Domain and hosting infrastructure built for resilience, not for a cleaning-game brand |

## What We Predicted, and What Happened

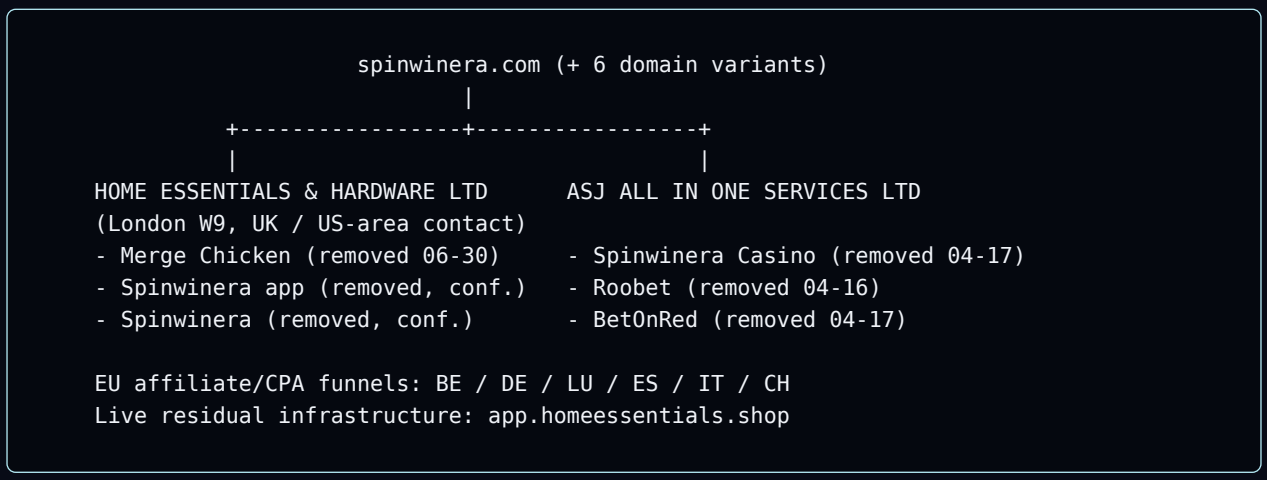
The MERGECHICKEN-001 report closed with this residual-risk note: "A takedown removes the listing, not the actor. The developer account HOME ESSENTIALS & HARDWARE LIMITED also operates 'Spinwinera', and the gambling payload is served from spinwinera.com - infrastructure that survives the removal of any single package."

**Confirmed - and larger than predicted**

The prediction named one sibling app. Investigation found a second developer account entirely, running three more listings under the same casino brand, plus a domain constellation and a prior, unattributed enforcement history. Both accounts are now confirmed actioned.

## The Network, Not Just the App

A casino domain used as an app's own brand name was already a strong signal on a single account. Finding the identical brand reused across a second, nominally unrelated developer account turns an app-level finding into an operator-level one. ASJ ALL IN ONE SERVICES LIMITED's three listings (Spinwinera Casino, Roobet, BetOnRed) were already removed by Google in April 2026 - a prior enforcement action against the same brand family that had gone unattributed to the Merge Chicken operator until this investigation connected the two accounts.




## Findings

### SW-01: Two-account operator network built on one casino brand

**CRITICAL - Multi-account repeat-offender, single-operator control**

Two distinct Play developer accounts distributed apps named after or linked to the same casino brand: HOME ESSENTIALS & HARDWARE LIMITED (Merge Chicken, Spinwinera app, Spinwinera) and ASJ ALL IN ONE SERVICES LIMITED (Spinwinera Casino, Roobet, BetOnRed). A shared casino brand deployed across two nominally-unrelated developer accounts is single-operator control expressed as account-level evasion.

```
Account 1: HOME ESSENTIALS & HARDWARE LIMITED (342 Kilburn Lane, London W9 3EF, UK)
  - com.Merge.o98Chickens        "Merge Chicken"        removed 2026-06-30
  - com.win.era.appofficial      "Spinwinera app"       removed (confirmed 2026-07-07)
  - com.spinwinera.app           "Spinwinera"           removed (confirmed 2026-07-07)

Account 2: ASJ ALL IN ONE SERVICES LIMITED
  - com.astrovanakatoryhnelzyazhitnelyaohhh  "Spinwinera Casino"  removed 2026-04-17
  - com.zhutkiestatuiZhutzhutstat            "Roobet"             removed 2026-04-16
  - com.konzertykotoryevocshlivistoriyuKonKOnvik "BetOnRed"        removed 2026-04-17

Shared brand / C2: spinwinera.com, spinwinera.org, spin-winera.net, spinwinera.ca,
spinwinera-de.com, spinwineracasino.org, spinwineracasino.net
EU affiliate/CPA funnels observed: BE / DE / LU / ES / IT / CH
```

**Impact:** This is not one app or one account; it is a casino-shell factory operating across at least two incorporated fronts, six package identities, and a seven-domain constellation. Google's own April 2026 mass-removal of the ASJ account's listings, followed by June-July action against the HOME ESSENTIALS account, shows the operator survives individual take-downs by re-incorporating and re-listing under a new account.

**SW-02: Bespoke anti-emulator / anti-sandbox detection in a children's cleaning game**

**CRITICAL - Deliberate review/analysis evasion (binary-confirmed)**

Independent decompilation of com.win.era.appofficial recovered explicit sandbox-fingerprinting logic with no legitimate purpose in a cleaning-game app: emulator manufacturer/brand matching, Houdini ARM-translation detection, a light-sensor-missing check, and an explicit BlueStacks package check.

```
"Device supports x86 ABIs (Common for Emulators)"
"Emulator Manufacturer/Brand match"
"Houdini ARM-translation detected (Emulator signature)"
"Light sensor missing"
com.bluestacks.app  <- explicit package check

casino URL: not present in binary. dormant UniWebView + OpenUrl path present,
points to no in-binary destination -> destination injected at runtime,
survives static review (same evasion class as Merge Chicken's Firebase Remote Config).
```

**Impact:** A real cleaning game has no reason to detect BlueStacks or emulator ABIs. This is purpose-built review evasion, binary-confirmed independent of the account-linkage ar-

gument, and demonstrates the same runtime-injection facade already proven on Merge Chicken generalizes to a design pattern, not a one-off.

**SW-03: Live, unlicensed real-money casino and sportsbook at the shared domain**

---

**CRITICAL - Unlicensed real-money gambling, no KYC**

spinwinera.com, the brand both accounts' listings are named after, operates as a full real-money casino and sportsbook: Pragmatic Play, BGaming and Evolution live-dealer roulette, Bitcoin and card deposits, a EUR 1,500 welcome bonus, and no Know-Your-Customer process beyond a self-declared date of birth.

**Impact:** The same no-KYC, real-money exposure documented in MERGECHICKEN-001 (MC-03) is confirmed live at the shared casino domain every listing in this network points back to, with EU affiliate/CPA funnels observed across six member states.

**SW-04: Age-rating contradiction across the network**

---

**HIGH - Age-rating circumvention (minor protection)**

Multiple listings in this network (Merge Chicken, Spinwinera app) carry PEGI 3 ("suitable for all ages") or similarly benign store ratings, while the casino brand they connect to restricts access to 18+ in its own site footer.

**Impact:** Repeats, at network scale, the age-rating circumvention established in MERGECHICKEN-001 (MC-02): all-ages storefront listings sitting in front of a product the operator's own site admits is 18+ only.

**SW-05: Corporate identity inconsistency - UK-registered front, US contact number**

---

**HIGH - Beneficial-ownership / attribution anomaly**

HOME ESSENTIALS & HARDWARE LIMITED lists a London W9 registered address and o rders@homeessentialshardware.uk as its support contact, but its listed contact phone number (+1 918-329-0460) resolves to an Oklahoma, US area code — a jurisdictional mismatch inconsistent with a genuine UK home-goods trading business.

```
Registered address : 342 Kilburn Lane, London W9 3EF, United Kingdom
Support email      : orders@homeessentialshardware.uk
Listed phone       : +1 918-329-0460  (Tulsa, Oklahoma, US area code)
Live cover site    : app.homeessentials.shop (still live)
```

**Impact:** A UK-incorporated entity operating a real-money gambling scheme with a US-area-code contact number and no coherent single jurisdiction of operation is a standard benefici al-ownership obfuscation pattern, and is the kind of inconsistency that warrants Companies House / NCA follow-up independent of the Play Store enforcement outcome.

**SW-06: Domain and hosting infrastructure built for resilience, not for a cleaning-game brand**

**HIGH - Bulletproof / redundant infrastructure**

The casino brand is mirrored across seven domain variants spanning at least four TLD families (.com, .org, .net, .ca) plus a country-coded variant (spinwinera-de.com), a redundancy pattern built for takedown resilience rather than the footprint of a single storefront cleaning-game app.

**Impact:** Multi-domain redundancy lets the operator survive individual domain seizures or registrar action; registrars and hosting providers, not only the Play Store, are a relevant enforcement surface for the underlying infrastructure.

## Impact Analysis

Minors. Every all-ages listing in this network (Merge Chicken, Spinwinera app) sits directly in front of a real-money casino with no age verification beyond a self-declared date of birth. A child who installs any of these apps can reach live gambling and Bitcoin deposit flows.

Financial & consumer. Across six confirmed app listings and a seven-domain hosting constellation, the operator ran an unlicensed money-handling channel at meaningfully larger scale than a single app - with EU affiliate/CPA funnels actively driving traffic into it from at least six member states (Belgium, Germany, Luxembourg, Spain, Italy, Switzerland).

Anti-money-laundering and corporate structuring. Two separate UK-registered entities distributing the identical casino brand, one of them re-emerging after a prior enforcement action against the other's sibling listings, is consistent with deliberate corporate layering to survive individual account or company-level enforcement - a structuring pattern of interest well beyond app-store policy.

Data protection. To the extent EU/EEA users were reached via any of the six listings or the affiliate funnels into BE/DE/LU/ES/IT/CH, the processing of financial and behavioural data engages GDPR Art. 5/6/7 (lawfulness, consent) and Art. 8 (minors), consistent with the same engagement already documented for Merge Chicken.

## The Complete Chain: Listing to Loss, at Network Scale

Each stage below is independently benign-looking and individually deniable; together, replicated across six listings and two incorporated fronts, they describe a scaled operation rather than an isolated app.

| Stage | Mechanism | Norm engaged |
|---|---|---|
| 1. Incorporation | Two UK-registered fronts (HOME ESSENTIALS & HARDWARE LTD, ASJ ALL IN ONE SERVICES LTD), one with a US-area contact number | Beneficial-ownership transparency; Companies House filing accuracy |
| 2. Discovery | All-ages listings, casual-game categories, neutral or casino-branded names across six packages | Age-rating system; Google Play families policy |

| Stage | Mechanism | Norm engaged |
|---|---|---|
| 3. Review evasion | Runtime-injected payload (Merge Chicken) or bespoke anti-sandbox fingerprinting (Spinwinera app) | Play deceptive-behaviour & dynamic-payload policy |
| 4. Activation / redundancy | Seven-domain constellation across four TLD families backing one casino brand | GDPR Art. 13/14 (undisclosed processing); domain-abuse policy |
| 5. Traffic acquisition | EU affiliate/CPA funnels observed in six member states | Cross-border consumer protection; gambling advertising law |
| 6. Onboarding | No age check, no KYC beyond self-declared DOB | UK Gambling Act 2005; AML (MLR 2017 / AMLD) |
| 7. Payment | Bitcoin and card deposits, EUR 1,500 bonus hook | UCPD dark patterns; AML crypto on/off-ramp exposure |
| 8. Persistence after enforcement | ASJ account re-emerges under the same brand after April 2026 removals; HOME ESSENTIALS cover site remains live | Repeat-offender / account and corporate evasion |

## Financial Crime & Cross-Border Anti-Money-Laundering

An online casino accepting real-money and cryptocurrency deposits without a licence and without Know-Your-Customer is, by construction, a money-handling channel operating outside the anti-money-laundering perimeter. Run across two corporate fronts and a multi-domain hosting constellation, with active EU affiliate funnels in six member states, the scale here is materially larger than a single-app case.

- EU: 4th/5th/6th Anti-Money-Laundering Directives bring providers of gambling services within scope; an unlicensed operator collecting deposits across two fronts sidesteps the entire CDD regime in every jurisdiction the affiliate funnels reach.
- UK: the Money Laundering Regulations 2017 and the Proceeds of Crime Act 2002 impose CDD and reporting duties on UK-incorporated entities; two UK-registered companies running the same unlicensed casino brand is a structuring pattern worth NCA attention.
- Bitcoin deposits alongside card deposits give the operator both a traceable-in-principle rail and a less traceable one; the combination is typical of operations optimising for payment-rail redundancy over compliance.
- Corporate re-emergence after enforcement (ASJ's April 2026 removals, followed by continued operation of the same brand under HOME ESSENTIALS) is consistent with using multiple shells specifically to survive individual company- or account-level action.
- EU affiliate/CPA funnels into BE/DE/LU/ES/IT/CH indicate active, paid customer acquisition into an unlicensed gambling product across at least six national markets simultaneously.

## Corporate Structure & Beneficial Ownership

Two UK-registered entities - HOME ESSENTIALS & HARDWARE LIMITED and ASJ ALL IN ONE SERVICES LIMITED - distributed apps built around the identical casino brand and domain constellation. Neither entity's registered trading description (household goods; general services) bears any relationship to real-money gambling, a mismatch consistent with the use of incorporated shells as a publishing front rather than the entities' stated business.

| Signal | Detail | Why it matters |
|---|---|---|
| Trading-name mismatch | "Home Essentials & Hardware" / "ASJ All In One Services" - neither name relates to gambling | Classic shell-front naming; obscures the actual business from cursory registry review |
| Jurisdictional inconsistency | UK registered address, but support phone number resolves to Oklahoma, US | Beneficial owner or operations base likely outside the UK despite UK incorporation |
| Live cover site | app.homeessentials.shop still live and presenting as a legitimate storefront | Active attribution cover maintained even after all Play Store listings are removed |
| Re-emergence after enforcement | ASJ's three listings removed April 2026; brand continues operating under HOME ESSENTIALS until July 2026 | Multi-entity structuring to survive single-company enforcement action |

None of the foregoing is a determination of who ultimately controls either entity. It is offered as a structured attribution package for whichever authority - Companies House, the NCA, or an EU financial-intelligence unit - is positioned to pursue beneficial-ownership verification.

## Child Protection & Developmental Harm

The gravest dimension of this network is not corporate or technical. Multiple listings carried an all-ages rating while sitting in front of a real-money casino reachable with a typed-in age and, in at least one listing, Bitcoin deposit. Gambling mechanics are engineered to exploit reward circuitry; deploying them to children across six separate listing surfaces, with no age assurance and no spending limits, is a child-safety failure that scales with the size of the network.

- UN Convention on the Rights of the Child: Art. 3 (best interests), Art. 32/36 (protection from economic exploitation).
- UK Age Appropriate Design Code (Children's Code) and the EU Better Internet for Kids / AVMSD expectations on age assurance and against nudging toward harmful behaviour.
- GDPR Art. 8 (conditions for a child's consent in information-society services) - defeated by self-declaration across every listing in the network.
- Gambling-by-design exposure to minors, replicated across two corporate fronts and six listings, is the kind of harm that draws coordinated child-protection, gambling and data-protection scrutiny simultaneously - and at greater scale than a single app.

## Consumer Protection & Deceptive Design

Three deceptions operate at once across this network: the listings misrepresent the product (a casino sold as children's or utility apps), the corporate registration misrepresents the business (household-goods and general-services entities actually running gambling), and the domain constellation misrepresents durability (redundant hosting built to survive enforcement rather than to serve one honest brand).

- EU Unfair Commercial Practices Directive 2005/29/EC: misleading actions (false age ratings / product nature / corporate identity) across every listing in the network.
- Aggressive practices: EU affiliate/CPA funnels driving paid acquisition into an unlicensed gambling product across six member states simultaneously.
- Austria: UWG (unlauterer Wettbewerb) and KSchG (consumer protection) for marketing to and contracting with AT consumers reached via any of the network's domains or funnels.
- No withdrawal rights, no transparent pricing, no functioning complaint path across any listing - users have none of the protections a lawful purchase or a licensed gambling product carries.

## Data Protection - Article by Article

To the extent EU/EEA users were reached - directly through any of the six listings, or through the EU affiliate/CPA funnels into BE/DE/LU/ES/IT/CH - the GDPR engagement is broad and concrete, and repeats across every listing in the network.

| Article | Obligation | How it is engaged |
|---|---|---|
| Art. 5(1)(a) | Lawfulness, fairness, transparency | Product nature and processing concealed behind game/utility facades across six listings |
| Art. 6 / 7 | Lawful basis / valid consent | No CMP or valid consent basis established for casino-adjacent processing |
| Art. 8 | Children's consent | Self-declared age across every listing; minors reach real-money processing |
| Art. 13 / 14 | Transparency of processing & recipients | Casino payload / cross-domain data flows undisclosed at store-listing level |
| Art. 25 | Data protection by design & default | No minimisation; redundant multi-domain infrastructure by design |
| Art. 32 | Security of processing | No verified security posture for financial/deposit data across the network |

## Payment Rails & Financial Infrastructure

- Bitcoin deposits alongside card deposits give this operator two independent payment rails - one with pseudonymous on-chain traceability, one governed by card-scheme rules the

operator is not licensed to sit within.

- A EUR 1,500 welcome bonus is a customer-acquisition mechanism typical of licensed operators, deployed here without a licence - the incentive structure of regulated gambling without any of its consumer safeguards.
- Unlicensed operators handling both fiat card rails and cryptocurrency on/off-ramps outside a compliant processor relationship raise liability across both the acquiring chain and any crypto exchange or wallet provider unknowingly facilitating deposits/withdrawals.
- No public information indicates a licensed payment processor or gambling-authority relationship for either corporate front; the payment infrastructure sits entirely outside supervised channels.

## Platform Accountability & the DSA

The scheme depends on distribution platforms and hosting/registrar infrastructure. Google Play's Developer Programme Policy prohibits real-money gambling outside a licensed, geo-restricted, age-gated framework, prohibits deceptive behaviour, and prohibits dynamic code loading and sandbox-evasion techniques that change app behaviour in violation of policy - all independently engaged across this network's six listings. Under the EU Digital Services Act, an intermediary of this scale carries notice-and-action and systemic-risk obligations; a coordinated, cross-account researcher report of this kind is precisely the trusted-flagger signal the DSA framework is designed to action. Confirmation of both accounts within the same sixteen minutes shows the mechanism scales from a single app to a multi-account network when the signal is precise and structured.

## Domain & Hosting Infrastructure

The casino brand is mirrored across at least seven domains spanning four TLD families, a redundancy pattern built for resilience against individual domain seizure rather than the footprint a single storefront app would need.

| Domain | Role |
|---|---|
| spinwinera.com | Primary casino domain; runtime C2 for Merge Chicken's Firebase Remote Config payload |
| spinwinera.org | Domain-constellation variant |
| spin-winera.net | Domain-constellation variant (hyphenated) |
| spinwinera.ca | Domain-constellation variant (Canada ccTLD) |
| spinwinera-de.com | Country-targeted variant (Germany) |
| spinwineracasino.org | Domain-constellation variant |
| spinwineracasino.net | Domain-constellation variant |
| app.homeessentials.shop | Live storefront cover site, HOME ESSENTIALS & HARDWARE LIMITED attribution (residual, out of Play Store scope) |

- Registrars and hosting providers for the spinwinera.* constellation and app.homeessentials.shop are a relevant enforcement surface independent of the Play Store outcome.

- A brand mirrored across seven domains and two corporate fronts is a durable identifier that outlives any single takedown; standing detection against the domain constellation, not just the package IDs, is recommended.

## Potential Criminal Exposure

The following is presented strictly as analysis for the competent authorities and prosecutors; it is not a legal determination and asserts no individual guilt.

- UK Gambling Act 2005: providing or advertising facilities for gambling without an operating licence is a criminal offence (s. 33) - potentially engaged by both UK-registered entities.
- Fraud: misrepresenting an 18+ real-money casino as all-ages games or household-goods/general-services businesses, combined with a US-area contact number inconsistent with the UK registration, may engage UK Fraud Act 2006 (fraud by false representation) and, for AT consumers reached via the network, StGB Section 146 (Betrug).
- Proceeds of Crime Act 2002 / conspiracy: two coordinated corporate fronts distributing the identical unlicensed gambling brand, with one re-emerging after the other's enforcement, is consistent with a structured conspiracy rather than independent, coincidental conduct - a framing for the competent authorities to assess.
- Data offences: unlawful processing of minors' and payment data across six listings may engage national criminal data-protection provisions in each jurisdiction reached.
- The corporate-front pattern (two UK shells, one seven-domain hosting constellation, one live cover site) is precisely the kind of structure that warrants beneficial-ownership and cross-border review by the NCA or an equivalent authority.

**Note**

RFI-IRFOS makes no determination of guilt. These framings exist so that the competent gambling, consumer, data-protection, financial-crime and law-enforcement authorities can each assess the conduct within their own remit on a complete factual record.

## Regulatory & Legal Landscape

The following framings are presented as analysis for the competent authorities; they are not legal determinations.

| Authority / regime | Jurisdictional hook | Potential basis |
|---|---|---|
| Google Play (platform) | App distribution, two accounts | Real-money gambling, deceptive behaviour, dynamic-payload and sandbox-evasion policy |
| UK Companies House / NCA | Both entities UK-registered | Beneficial-ownership verification; structuring across two fronts |

| Authority / regime | Jurisdictional hook | Potential basis |
|---|---|---|
| UK Gambling Commission | Both developers UK-established | Gambling Act 2005 - providing/advertising facilities for gambling without a licence |
| UK ICO | UK-established controllers | UK GDPR - payment data security, children's data, across six listings |
| Austrian DSB | EU/AT data subjects reached | GDPR Art. 5/6/8/32 |
| EU consumer / UCPD bodies (BE/DE/LU/ES/IT/CH) | Affiliate/CPA funnels observed in each state | Unfair commercial practices; cross-border gambling advertising |
| Domain registrars / hosts | Seven-domain constellation | Abuse-policy action against the spinwinera.* family and app.homeessentials.shop |
| Card schemes / crypto exchanges | Bitcoin and card deposit rails | Unlicensed gambling payment handling outside supervised channels |

## Indicators of Compromise

| Type | Value |
|---|---|
| Package (Account 1) | com.Merge.o98Chickens - "Merge Chicken" (PEGI 3) - removed 2026-06-30 |
| Package (Account 1) | com.win.era.appofficial - "Spinwinera app" - removed, confirmed 2026-07-07 |
| Package (Account 1) | com.spinwinera.app - "Spinwinera" - removed, confirmed 2026-07-07 |
| Package (Account 2) | com.astrovanakatoryhnelzyazhitnelyaohhh - "Spinwinera Casino" - removed 2026-04-17 |
| Package (Account 2) | com.zhutkiestatuiZhutzhutstat - "Roobet" - removed 2026-04-16 |
| Package (Account 2) | com.konzertykotoryevocshlivistoriyuKonKOnvik - "BetOnRed" - removed 2026-04-17 |
| Base APK SHA-256 (Merge Chicken) | d207fe2ba3a051c298ff60d1487a184cc2f05f8edb2321d3ef14c9f140a3f62b |
| Base APK SHA-256 (Spinwinera app) | 7d7dd2b31ac21545ae95e9e20db12bd6f2c087065896e540483f338eda0c16ec |
| C2 / brand domain | spinwinera.com |
| Domain constellation | spinwinera.org, spin-winera.net, spinwinera.ca, spinwinera-de.com, spinwineracasino.org, spinwineracasino.net |
| Live residual site | app.homeessentials.shop |
| Developer entity 1 | HOME ESSENTIALS & HARDWARE LIMITED, 342 Kilburn Lane, London W9 3EF, UK |

| Type | Value |
|---|---|
| Developer entity 1 contact | orders@homeessentialshardware.uk; phone +1 918-329-0460 (Oklahoma, US - jurisdictional mismatch) |
| Developer entity 2 | ASJ ALL IN ONE SERVICES LIMITED |
| EU affiliate/CPA funnel markets | Belgium, Germany, Luxembourg, Spain, Italy, Switzerland |

## Disclosure Timeline & Outcome

| Date | Event |
|---|---|
| 2026-04-16/17 | (Retrospectively attributed) ASJ ALL IN ONE SERVICES LIMITED's Spinwinera Casino, Roobet and BetOnRed removed by Google - unattributed to this operator at the time. |
| 2026-06-25 | MERGECHICKEN-001 reported to Google Play & Android Security. |
| 2026-06-30 | Merge Chicken confirmed removed. Google invites further leads. |
| 2026-07-01 | Three coordinated reports filed same day: SPINWINERA-001 (fresh lead), SPINWINERA-A (binary analysis of com.win.era.appofficial), SPINWINERA-B (cross-account attribution to ASJ ALL IN ONE SERVICES LIMITED). |
| 2026-07-01 | All three acknowledged by the Play and Android Security Team within hours. |
| 2026-07-07 05:18 UTC | SPINWINERA-001 confirmed: "We can now confirm that the apps are no longer available on the Play Store." |
| 2026-07-07 05:34 UTC | SPINWINERA-B confirmed, identical wording, covering the ASJ ALL IN ONE SERVICES LIMITED account. |

**Outcome**

Six app listings across two developer accounts, all built around the same casino brand, are confirmed off the Google Play Store. Third and fourth confirmed enforcement outcomes of the RFI-IRFOS 2026 Android audit programme, six days from the follow-on reports to resolution.

## What This Confirms About the Evasion Class

Two things generalize from Merge Chicken rather than being unique to it. First, runtime-injected or behaviourally-cloaked payloads that pass static review are a repeatable design pattern, not a one-off - independently re-confirmed on com.win.era.appofficial through a different technical signature (anti-sandbox fingerprinting rather than a hardcoded C2 string). Second, actor-level and brand-level linkage - shared casino name, shared domain constellation, shared shell-game construction, shared corporate irregularities - is sufficient for the platform to act on even where a fresh full decompile has not been completed, and even across accounts nominally unconnected on paper.

- Re-offending operators should be tracked at the brand/domain level across accounts, not solely at the individual-package or individual-account level.
- Anti-emulator/anti-sandbox fingerprinting inside a game with no legitimate reason to check for BlueStacks is, on its own, a strong static indicator of review evasion.
- A prior, previously-unattributed platform enforcement action (the April 2026 ASJ removals) can retroactively become part of a coherent operator profile once a connecting brand is identified.
- Corporate-registry inconsistencies (mismatched trading name, jurisdiction, contact number) are a durable attribution signal that survives both app-level and account-level takedowns.

## Residual Risk & Recommendations

All six identified app listings across both accounts are now confirmed off the Play Store. One artifact remains live and outside Play Store enforcement scope: app.homeessentials.shop, a legitimate-looking storefront website operated as attribution cover for HOME ESSENTIALS & HARDWARE LIMITED. It is not itself a Play Store listing and is flagged for awareness rather than platform action.

**Open**

app.homeessentials.shop remains live. It is out of Google Play & Android Security's remit; any action on it would fall to a domain registrar, hosting provider, or a consumer-protection/financial-crime authority. Tracked as an open item on the public ledger.

- Platform: treat the spinwinera.* domain constellation and the Roobet/BetOnRed brand names as standing abuse indicators regardless of the publishing account.
- Registrars/hosting: app.homeessentials.shop and the seven-domain spinwinera.* constellation warrant independent review as operator-attribution infrastructure surviving app-level and account-level takedowns.
- Companies House / NCA: the mismatched trading names, the US-area contact number on a UK-registered entity, and the two-shell re-emergence pattern warrant beneficial-ownership follow-up independent of the Play Store outcome.
- EU consumer/gambling bodies (BE/DE/LU/ES/IT/CH): the affiliate/CPA funnels observed in each market indicate active, paid customer acquisition into an unlicensed gambling product reaching each jurisdiction.
- General: cross-account, cross-domain and cross-corporate brand reuse is a durable identifier that outlives any single incorporation, package ID or domain - worth a standing detection rule independent of any single reporter.

**RFI-IRFOS** rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria This matter was reported directly to the platform as abuse; no commercial engagement was offered. Binary evidence for MERGECHICKEN-001 and SPINWINERA-A is archived under chain of custody and available to regulatory authorities on request.

The SPINWINERA-001 and SPINWINERA-B linkage evidence (shared account, shared brand, shared domain constellation, corporate-registry analysis) is presented as reported to Google Play & Android Security; independent binary confirmation of those specific packages was not performed prior to takedown, and the corporate/financial-crime framing is desk analysis for the competent authorities, not a legal determination. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF SPINWINERA-001/A/B.