Security Disclosure & Takedown Report

Merge Chicken

com.Merge.o98Chickens - a PEGI 3 “children’s game” operating an unlicensed, no-KYC real-money casino

RESOLVED • REMOVED FROM THE GOOGLE PLAY STORE

Analyst	RFI-IRFOS Research Team
Report date	2026-06-30
App version	1.0.2 (versionCode 3)
Package	com.Merge.o98Chickens
Play rating	PEGI 3 (suitable for all ages)
Developer	HOME ESSENTIALS & HARDWARE LIMITED, London W9 3EF, UK
Severity	CRITICAL
Findings	6 (6 CRITICAL)
Reported	2026-06-25 - Google Play & Android Security
Resolved	2026-06-30 - removed from the Play Store
Time to outcome	5 days

SHA-256 (base APK):

`d207fe2ba3a051c298ff60d1487a184cc2f05f8edb2321d3ef14c9f140a3f62b`

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

"Merge Chicken" (com.Merge.o98Chickens) was distributed on Google Play under a PEGI 3 ("suitable for all ages") rating, presented as a casual merge puzzle game. Root-level analysis of the distributed Android binary established that the application functioned as an unlicensed, no-KYC real-money online casino, with its gambling functionality delivered dynamically at runtime so that the build submitted for store review did not, on its face, contain it.

This was not a privacy-policy dispute with a legitimate operator. It was a deceptive, financially-motivated scheme that placed a real-money gambling product in front of an all-ages audience, captured payment-card data through dark patterns, accepted deposits without any identity or age verification, and transmitted financial data in cleartext. Accordingly, the matter was not handled as a commercial coordinated-disclosure engagement and no remediation offer was made; it was reported directly to Google Play & Android Security as abuse, and referred to the competent regulators.

Scope: Static root-level analysis of the published release APK using apktool, dex/string inspection and manifest review, plus open-source corroboration of the developer entity. No production servers or user accounts were probed. Evidence is archived under chain of custody and available to competent authorities on request.

Disposition

Reported to Google Play & Android Security on 2026-06-25. Receipt acknowledged the same day. On 2026-06-30, the Play and Android Security Team confirmed: "We can now confirm that the app is no longer available on the Play Store." Time to resolution: 5 days. This is the first publicly documented enforcement outcome of the RFI-IRFOS 2026 Android audit programme.

ID	Severity	Title
MC-01	CRITICAL	Cloaked gambling - dynamic payload via Firebase Remote Config (C2: spinwinera.com)
MC-02	CRITICAL	PEGI-3 bypass - 18+ real-money casino on an all-ages listing
MC-03	CRITICAL	No-KYC real-money gambling - deposits without identity or age verification
MC-04	CRITICAL	Pre-checked payment-card storage (dark pattern)
MC-05	CRITICAL	CVV capture on stored-card flow
MC-06	CRITICAL	Cleartext HTTP for transaction / payment traffic

Subject & Threat-Actor Analysis

The Play developer account of record is HOME ESSENTIALS & HARDWARE LIMITED (342 Kilburn Lane, London W9 3EF, United Kingdom; support contact orders@homeessentials hardware.uk). The trading name - a generic "hardware" company - bears no relationship to either a casual game or a gambling operation, a pattern consistent with the use of an incorporated shell as a publishing front.

The same developer account also operates a second Play Store application, "Spinwinera". The gambling payload observed in Merge Chicken is served from the domain spinwinera.com. The shared brand and infrastructure across two listings indicate a coordinated operation rather than an isolated app, and a brand ("Spinwinera") that exists independently of the "Merge Chicken" facade.

Assessment

The configuration is characteristic of a deliberate storefront-evasion scheme: a benign-looking, age-neutral game is used to obtain an all-ages Play listing and pass automated review, while the actual revenue-generating product - an online casino - is delivered to the device from separately-controlled infrastructure after installation. The age rating, the store category and the developer identity each serve to distance the listing from the conduct it enables.

Architecture & Attack Surface

The defining technical property of this application is runtime cloaking via remote configuration. The store-reviewed binary does not statically present as a casino; the gambling experience is gated behind, and delivered through, a server-controlled switch.

Because the casino is enabled by remote configuration, the operator retains the ability to keep the gambling surface dormant during store review and enable it afterwards, to target the rollout by geography or cohort, and to withdraw it on demand. This is the same evasion class that Google Play policy explicitly prohibits under its restrictions on deceptive behaviour and dynamic code loading that changes app behaviour in violation of policy.

Findings

MC-01: Cloaked gambling - dynamic payload via Firebase Remote Config (C2: spinwinera.com)

CRITICAL - Deceptive behaviour / dynamic payload (Google Play Policy; CWE-913)

The real-money gambling experience is not present as a static feature of the reviewed build. It is delivered at runtime through Firebase Remote Config, with command-and-control to spinwinera.com, allowing an all-ages "merge game" listing to operate as an online casino.

```
mechanism : Firebase Remote Config (server-controlled feature gating)
C2 / payload host : spinwinera.com
facade    : Play listing "Merge Chicken", category casual game, PEGI 3
```

Impact: The store-review safeguards, the age rating and the category are all defeated by design. Users - including minors - who install a children's game are served a gambling product controlled from external infrastructure.

MC-02: PEGI-3 bypass - 18+ real-money casino on an all-ages listing

CRITICAL - Age-rating circumvention / minor protection

An 18+ real-money gambling product was delivered through a listing rated PEGI 3 ("suitable for all ages"), defeating the age-rating system parents and the store rely upon.

Impact: Age ratings are a primary parental control. Presenting gambling under a PEGI 3 label is a direct circumvention of child-protection expectations and of Google Play's gambling and real-money-gaming policies, which require age-gating, licensing and geographic restriction.

MC-03: No-KYC real-money gambling - deposits without identity or age verification

CRITICAL - No identity / age verification (AML / minor protection)

The application accepts immediate real-money deposits with no Know-Your-Customer process and no age verification.

Impact: The absence of KYC exposes minors to direct financial loss and removes the controls that lawful, licensed gambling operators are obliged to operate (identity, age, source-of-funds, self-exclusion). It also creates anti-money-laundering exposure: an unlicensed money-handling flow with no customer due diligence.

MC-04: Pre-checked payment-card storage (dark pattern)

CRITICAL - Deceptive design / consent (CWE-451)

Payment-card storage is enabled by default (pre-checked), capturing card data absent an affirmative, informed user choice.

Impact: A pre-checked storage option is a recognised dark pattern; on a gambling product handling real money this maximises captured card data and undermines any claim of valid consent for the processing of that financial data.

MC-05: CVV capture on stored-card flow

CRITICAL - Improper handling of cardholder data

The application requests the card verification value (CVV), contrary to standard handling for stored-card flows, where the CVV must not be retained.

Impact: CVV capture in combination with stored card data (MC-04) is inconsistent with card-scheme handling rules and materially increases the value and risk of the captured payment dataset.

MC-06: Cleartext HTTP for transaction / payment traffic

CRITICAL - Missing transport encryption (CWE-319)

Transaction- and payment-related traffic is permitted over unencrypted HTTP, exposing financial data to interception.

Impact: Cleartext transmission of payment and transaction data allows interception and manipulation by any party on the network path (hostile Wi-Fi, on-path attacker), compounding every finding above by exposing the very data the scheme collects.

Impact Analysis

Minors. The combination MC-02 + MC-03 is the gravest: a child who installs an all-ages game can reach a real-money casino and deposit funds with no age check. The harm is immediate and financial, not abstract.

Financial & consumer. MC-03 + MC-04 + MC-05 + MC-06 together describe an unlicensed money-handling flow that maximises captured card data through a dark pattern, retains the CVV, and exposes it in transit. Affected users have none of the protections (dispute, self-exclusion, deposit limits, source-of-funds checks) that licensed gambling and regulated payment handling require.

Anti-money-laundering. An online casino operating without a licence and without KYC is, by construction, a money-handling channel without customer due diligence - a recognised AML risk vector.

Data protection. To the extent EU/EEA users were reached, the processing of payment data over cleartext (MC-06) and the pre-checked capture of card data (MC-04) engage GDPR

Art. 32 (security of processing) and Art. 5/6/7 (lawfulness, consent), and the processing of minors' data engages Art. 8.

The Complete Chain: Listing to Loss

A single mechanism is not the story; the story is the chain. Each stage is independently benign-looking and individually deniable, yet together they convert an all-ages app-store listing into financial loss for a user who may be a child. The table maps every stage to the technical mechanism that enables it and the norm it engages.

Stage	Mechanism	Norm engaged
1. Discovery	PEGI 3 listing, casual-game category, neutral name	Age-rating system; Google Play families policy
2. Review evasion	Casino absent from reviewed build; gated by Firebase Remote Config	Play deceptive-behaviour & dynamic-payload policy
3. Activation	Payload + UI fetched from spinwinera.com after install	GDPR Art. 13/14 (undisclosed processing); platform policy
4. Onboarding	No age check, no KYC	UK Gambling Act 2005; AML (MLR 2017 / AMLD)
5. Payment	Pre-checked card storage; CVV requested	UCPD dark patterns; PCI-DSS; GDPR Art. 7/25
6. Transmission	Cleartext HTTP	GDPR Art. 32; PCI-DSS Req. 4
7. Loss	Real-money deposit, no self-exclusion / limits	Consumer protection; gambling-harm duty of care

Financial Crime & Anti-Money-Laundering

An online casino that accepts real-money deposits without a licence and without Know-Your-Customer is, by construction, a money-handling channel operating outside the anti-money-laundering perimeter. There is no customer due diligence, no source-of-funds check, no transaction monitoring and no suspicious-activity reporting - the controls that licensed gambling operators and regulated payment institutions are obliged to run.

- EU: 4th/5th/6th Anti-Money-Laundering Directives bring providers of gambling services within scope; an unlicensed operator collecting deposits sidesteps the entire CDD regime.
- UK: the Money Laundering Regulations 2017 and the Proceeds of Crime Act 2002 impose CDD and reporting duties; remote gambling without a UKGC licence forfeits the supervised framework entirely.
- Card-not-present capture (pre-checked storage + CVV) on an unlicensed flow materially raises fraud and laundering exposure for the acquiring chain.
- The dynamic-payload design lets the operator switch the money-handling surface on and off by region - a structural obstacle to oversight.

Child Protection & Developmental Harm

The gravest dimension is not technical. A PEGI 3 label is a promise to a parent. Behind it sat a real-money casino reachable with a typed-in age and a stored card. Gambling mechanics are engineered to exploit reward circuitry; deploying them to children, with no age assurance and no spending limits, is a child-safety failure before it is a compliance failure.

- 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 nudge toward harmful behaviour.
- GDPR Art. 8 (conditions for a child's consent in information-society services) - defeated by self-declaration.
- Gambling-by-design exposure to minors is the kind of harm that draws coordinated child-protection, gambling and data-protection scrutiny simultaneously.

Consumer Protection & Deceptive Design

Two deceptions operate at once: the listing misrepresents the product (a casino sold as a children's game), and the payment flow uses dark patterns to extract card data. Both are squarely within unfair-commercial-practices law.

- EU Unfair Commercial Practices Directive 2005/29/EC: misleading actions (false age rating / product nature) and aggressive practices.
- Dark-pattern taxonomy: pre-selection (pre-checked card storage) and sneaking - explicitly targeted by EU consumer-law enforcement and the EU Digital Fairness agenda.
- Austria: UWG (unlauterer Wettbewerb) and KSchG (consumer protection) for marketing to and contracting with AT consumers.
- No withdrawal rights, no transparent pricing, no functioning complaint path - the user has none of the protections a lawful purchase carries.

Data Protection - Article by Article

To the extent EU/EEA users were reached, the GDPR engagement is broad and concrete.

Article	Obligation	How it is engaged
Art. 5(1)(a)	Lawfulness, fairness, transparency	Product nature and processing concealed behind a game facade
Art. 6 / 7	Lawful basis / valid consent	Pre-checked card capture is not freely-given consent
Art. 8	Children's consent	Self-declared age; minors reach real-money processing
Art. 13 / 14	Transparency of processing & recipients	spinwinera.com payload / data flows undisclosed
Art. 25	Data protection by design & default	Default-on card storage; no minimisation

Article	Obligation	How it is engaged
Art. 32	Security of processing	Cleartext HTTP for payment/transaction data

Payment-Card Security (PCI-DSS)

- PCI-DSS Req. 3.2: the card verification value (CVV) must not be stored after authorisation - capturing/retaining it on a stored-card flow is a direct prohibition breach.
- PCI-DSS Req. 4: cardholder data must be encrypted in transit over open networks - cleartext HTTP (MC-06) fails this outright.
- Pre-checked storage maximises the cardholder-data footprint while undermining the consent basis for holding it.
- An unlicensed operator handling card data outside a compliant processor relationship raises liability across the acquiring chain.

Platform Accountability & the DSA

The scheme depends on a distribution platform. Google Play's own Developer Programme Policy prohibits real-money gambling outside a licensed, geo-restricted, age-gated framework, prohibits deceptive behaviour, and prohibits dynamic code loading that changes app behaviour in violation of policy - each engaged here. Under the EU Digital Services Act, an intermediary of this scale carries notice-and-action and systemic-risk obligations; a coordinated researcher report is exactly the trusted-flagger signal the DSA framework is built to action. The five-day takedown shows the mechanism works when the signal is precise.

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).
- Fraud: misrepresenting an 18+ real-money casino as an all-ages game, combined with dark-pattern card capture, may engage UK Fraud Act 2006 (fraud by false representation) and, for AT consumers, StGB §146 (Betrug).
- Data offences: unlawful processing of minors' and payment data may engage national criminal data-protection provisions.
- The corporate-front pattern (a UK 'hardware' shell publishing gambling apps, second brand Spinwinera) is the kind of structure that warrants beneficial-ownership and cross-border review.

Note

RFI-IRFOS makes no determination of guilt. These framings exist so that the competent gambling, consumer, data-protection 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	Real-money gambling, deceptive behaviour, dynamic-payload policy
UK Gambling Commission	Developer established in the UK	Gambling Act 2005 - providing / advertising facilities for gambling without a licence
UK ICO	UK-established controller	UK GDPR - payment data security, children's data
Austrian DSB	EU/AT data subjects reached	GDPR Art. 5/6/8/32
EU consumer / UCPD	Marketing to EU consumers	Unfair commercial practices (deceptive design, age-rating misrepresentation)
Card schemes / acquirers	Card data handling	CVV retention, stored-card handling rules

Indicators of Compromise

Type	Value
Package	com.Merge.o98Chickens
App label	Merge Chicken (PEGI 3)
Version	1.0.2 (versionCode 3)
Base APK SHA-256	d207fe2ba3a051c298ff60d1487a184cc2f05f8edb2321d3ef14c9f140a3f62b
C2 / payload domain	spinwinera.com
Config mechanism	Firebase Remote Config
Developer entity	HOME ESSENTIALS & HARDWARE LIMITED, London W9 3EF, UK
Developer contact	orders@homeessentialshardware.uk
Linked app	"Spinwinera" (same developer account)

Disclosure Timeline & Outcome

Date	Event
2026-06-25	Abuse / malware report submitted to Google Play & Android Security (ISO/IEC 29147 coordinated disclosure).
2026-06-25	Receipt acknowledged by the Play and Android Security Team.
2026-06-30	Confirmation: "We can now confirm that the app is no longer available on the Play Store."
2026-06-30	Outcome recorded on the RFI-IRFOS permanent public disclosure ledger; competent regulators notified.

Outcome

The application was removed from the Google Play Store within five days of report. The listing-level threat is resolved.

Residual Risk & Recommendations

Residual risk. 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.

- Platform: action at the developer-account level (not only the single package); monitor for re-listing under new package identifiers; treat spinwinera.com as an abuse indicator across submissions.
- Gambling regulator (UK): assess unlicensed gambling provision / advertising by the UK-established developer.
- Data-protection authorities: assess payment-data security (cleartext) and processing of minors' data for EU/UK users.
- General: dynamic-payload cloaking via remote configuration is a repeatable evasion class and warrants review beyond this single listing.

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 All findings derive from static root-level analysis of the published application using publicly available tooling. No servers, accounts or infrastructure were probed. This matter was reported directly to the platform and referred to the competent authorities as abuse; no commercial engagement was offered. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF MERGECHICKEN-001.