

PRESS STATEMENT

Papaye, KFC and Pizzaman customers among most targeted as TrustGH uncovers nearly 1,000 scam numbers cloning Google Business Profiles of major food chains in Ghana

Accra, Ghana — 17 August 2026

TrustGH, Ghana's public scam-verification and reporting platform, has uncovered nearly 1,000 suspicious mobile numbers associated with fraudulent Google Business Profiles impersonating major food chains and restaurants in Ghana.

The findings follow an extensive open-source intelligence (OSINT) and digital investigation conducted by TrustGH, focusing specifically on the online presence of major food businesses on Google Search and Google Maps. The investigation examined suspicious business listings, telephone numbers and other publicly available digital indicators associated with suspected fraudulent restaurant profiles.

The investigation indicates that customers of Papaye, KFC and Pizzaman Chickenman are among the most heavily targeted, with close to 100 suspected fraudulent Google Business Profiles identified in connection with each of the three brands.

Other food businesses identified during the investigation include Pinkberry, Marwako, 80/20 Burger, Pizza Inn, Eddy's Pizza, Papa's Pizza, Noble House, Starbite, Chicken Inn, Pizza Hut, Burger King, Frankie's, Honeysuckle, Flicks & Licks, Chicken Republic and ChopShop.

A Digital Impersonation Threat

TrustGH's analysis indicates that scammers are exploiting the visibility and trust associated with established food brands by creating, modifying or manipulating Google Business Profiles to make them appear to be genuine restaurant branches.

Some of these profiles contain legitimate-looking business names, locations, photographs, menus, opening hours and other information copied from genuine businesses.

The critical security concern is the telephone number displayed on the fraudulent listing.

A customer searching for a nearby Papaye, KFC or Pizzaman outlet may see what appears to be an authentic business listing and call the number provided to place an order.

The person answering the call then provide accurate information about menus, prices, branches and ordering procedures. This can create a convincing customer-service interaction and significantly reduce the likelihood that the victim will suspect fraud.

The customer may subsequently be instructed to make payment through a mobile money number or payment link controlled by the suspected scammer.

From a cybersecurity perspective, this represents a form of digital identity and brand impersonation, in which criminals exploit trusted online business information to manipulate the victim into completing a fraudulent transaction.

Findings Based on OSINT and Digital Analysis

TrustGH's findings were developed through open-source intelligence gathering, digital investigation and analysis of publicly accessible information on Google.

The investigation focused on identifying anomalies and suspicious patterns surrounding food-business listings, including duplicated or suspicious profiles, telephone numbers, business information and other publicly observable indicators.

TrustGH stresses that the presence of a suspicious profile or telephone number does not, by itself, constitute conclusive proof of criminal activity. The findings represent risk indicators identified through OSINT and digital analysis, and individual cases require appropriate verification.

The number of suspicious listings may also change as fraudulent profiles are created, modified, suspended or removed.

Why Google Business Profiles Are Being Exploited

Google Search and Google Maps have become important tools for consumers looking for restaurants.

Customers can quickly identify a nearby branch, view opening hours, read reviews and obtain a telephone number without visiting the company's official website.

This convenience also creates an opportunity for criminals to exploit the digital information ecosystem.

TrustGH believes consumers should therefore understand that a business appearing on Google does not automatically mean that every piece of information displayed on the profile is authentic.

The telephone number on a fraudulent listing can become the bridge between an apparently legitimate online search and a fraudulent payment.

Nearly 5,000 Suspicious Numbers Reported

The food-chain investigation forms part of TrustGH's wider public database, which has received reports involving nearly 5,000 suspicious telephone numbers.

These reports cover mobile money scams, fake online sellers, fraudulent investment and banking schemes, fake recruitment offers, impersonation, social-media scams, loan scams, vehicle and property fraud, phishing and other suspicious activities.

The findings reinforce the importance of combining consumer awareness, digital investigation, public reporting and platform-level intervention to address online fraud.

TrustGH is calling for stronger collaboration among Google, affected businesses, the Cyber Security Authority and other relevant stakeholders to improve the detection, verification and removal of fraudulent business listings.

TrustGH Calls for Greater Verification

TrustGH is urging consumers to adopt a simple cybersecurity practice: **verify before you pay**.

Customers who find a restaurant through Google Search or Google Maps should independently verify the telephone number using the restaurant's official website, verified social-media account or another trusted channel before sending money.

Consumers are also encouraged to use **TrustGH.com** to check whether a suspicious telephone number has previously been reported.

If a number appears suspicious or is associated with a suspected scam, members of the public are encouraged to **report the number on TrustGH.com**. Public reporting can help build a broader intelligence picture and potentially warn other consumers.

Verify before you pay. Check suspicious numbers. Report suspected scams.

Visit: TrustGH.com

Issued by:

TrustGH

Public Scam Verification & Reporting Platform

Accra, Ghana