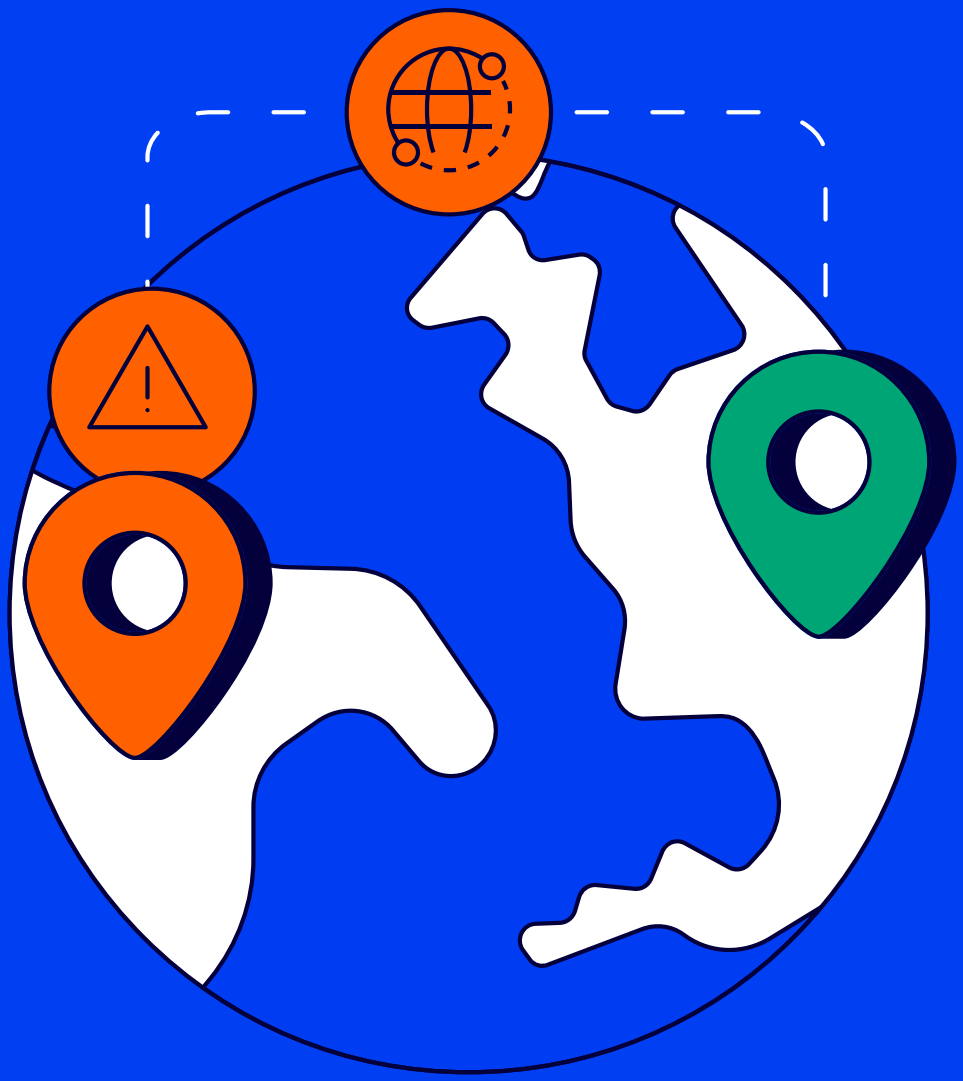
Geolocation intelligence for financial security

Using digital signatures to proactively detect and block “pig butchering” facilities



GeoComply

Table of Contents

Introduction

The internet has been essential for creating global communities. While this worldwide connectivity is responsible for significant social good, it has also created opportunities for bad actors. As the internet has grown, **criminal entities have become adept at using online platforms to find and target vulnerable populations.** In recent years, we have seen sophisticated transnational criminal gangs advance this trend through the development of a new scam typology known crudely as "pig butchering"

Pig butchering is a scam in which the perpetrator seeks to build emotional rapport with their victim over digital channels with the hope of fostering an online relationship. Once the victim's trust is gained, the scammer will incentivize the victim to invest in various schemes, often involving cryptocurrency. Victims will unknowingly transfer funds to a criminal organization, who will steal and launder the money.

Pig butchering is largely responsible for the post-Covid rise in financial scams. While the true scale of financial losses stemming from these scams is unknown (often due to victims' reluctance to report their exploitation), experts from the University of Texas estimate the total financial losses attributable to pig butchering from January 2020 to February 2024 is up to $75 Billion.[1] Often, this money comes out of the pockets of society's most vulnerable people.

Stopping scams and following the money

Pig butchering has two primary components: victim manipulation and the movement of funds. Strategies to combat pig butchering largely focus on the latter.

Since scammers primarily use cryptocurrencies to move money from their victims to themselves, financial institutions and law enforcement regularly use blockchain analytics tools to detect the movement of funds and assist law enforcement with asset recovery.[2]

However, blockchain analytics can only be one component of a robust anti-pig butchering defense. Additional technical solutions are needed to create digital protections for potential victims.

[1] Faux, Zeke. Pig-Butchering Scams Net More Than $75 Billion, Study Finds. Bloomberg. February 29, 2024
[2] The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed. Chainalysis. February 24, 2024

Proactive strategy for online communication platforms

While focusing on payment vectors is critical, it is just as important to prevent scammers from forming fraudulent relationships with their victims in the first place. While some of these fraudulent contractions are initiated over text, a considerable amount of fraudulent outreach occurs on mainstream dating applications and social media platforms.

> “According to research conducted by Ipsos and Aura, “12% of Americans who have used a dating app in the past five years have experienced “pig butchering”, which has also more than doubled from 5% over 5 years ago.”[3]
>
> **Aura**
> February 1, 2023

> “Scammers also take advantage of messaging features on large social media applications, such as Facebook, Instagram, and TikTok.[4]
>
> **Satnam Narang**
> February 14, 2024

These aforementioned platforms have a moral - if not legal - obligation to foster safe online environments. As the epidemic of online fraud grows, these companies need to take concrete steps to limit bad actors’ access to their platforms. Doing so requires them to take a proactive approach to analyzing suspicious behaviors and acting in response to distinct red flags.

[3] Scammers are Taking the Romance out of Valentine’s Day. Aura. February 1, 2023
[4] Narang, Satnam. Pig Butchering Scam: From Tinder and TikTok to WhatsApp and Telegram, How Scammers Are Stealing Millions in a Long Con. February 14, 2024

Cutting out the fraud factories

While many modern cybercriminal syndicates operate in a geographically dispersed fashion, the criminal gangs behind pig butchering scams operate out of concentrated facilities.

The reason for this centralization is disturbing. The proverbial foot soldiers of these scam operations are often trafficked and forced to perpetrate fraud against their will.[5]

This form of modern-day slavery requires gangs to hold their captives in secure facilities within jurisdictions with poor rule of law. While these prison camps turned "fraud factories" serve as the nerve centers for transnational gangs, they may also be the organizations' Achilles Heel.

The digital signatures associated with these fraud factories are detectable. Therefore, **the most obvious step for online platforms to improve their security is to block traffic originating from known illicit facilities.**

Major news outlets, including the New York Times[6] and Deutsche Welle[7], have reported on the specific locations of call centers. Online platforms can and should use this open-source information to geofence properties known to be tied to this illicit activity.

However, countering pig butchering is more complex than simply blocking known properties. Gangs will simultaneously take steps to obfuscate their associations with known pig butchering facilities, while also developing new facilities from which they can conduct fraud. For online platforms to engage in a truly effective anti-pig butchering strategy, they must have effective tools to stay ahead of bad actors' deceptive techniques. To do so, they need to understand some of the characteristics and incentives of these criminal gangs.

[5] Going undercover to expose life inside a scam centre - 'It's a fraud industry'. Sky News. October 18, 2024
[6] Qian, Isabelle. 7 Months Inside an Online Scam Labor Camp. The New York Times. December 17th, 2024
[7] Behind Asia's cyber slavery. Deutsche Welle. January 29, 2024

The three signals

High-risk countries

Anomalous concentrations of activity

Extensive utilization of location obfuscation tools

1 High risk countries

To reduce the likelihood of law enforcement intervention, the gangs will locate their facilities in jurisdictions with limited law enforcement capacity and poor rule of law.[8] Examples of such jurisdictions include the border regions of Myanmar, a country that has been in a state of civil war since a 2021 coup. Moreover, the border regions of Myanmar are generally dominated by rebel factions rather than the central government.[9] While Myanmar is far from the only country to host these facilities, it shares common characteristics, specifically poor rule of law, with other fraud factory host countries.

Online communications platforms seeking to proactively counter pig butchering need to look for spikes in activity in high-risk jurisdictions.

2 Anomalous concentrations of activity

For pig butchering to be profitable, the criminals need to pursue scale. Since many individuals will dismiss unsolicited contact, resulting in a low response rate, volume is key to fraudulent gains. It's not enough for one or two individuals to create a couple of accounts on a single platform. Criminal organizations require thousands of individuals to create thousands of accounts in order to be financially viable. The United Nations estimates that at least 120,000 people in Myanmar and 100,000 people in Cambodia have been trafficked into these online scam facilities.[10]

Not only do online platforms need to look for activity in high-risk areas; they also need to look for concentrations of accounts - especially if these concentrations seem disproportionate to the population density of a geographic area.

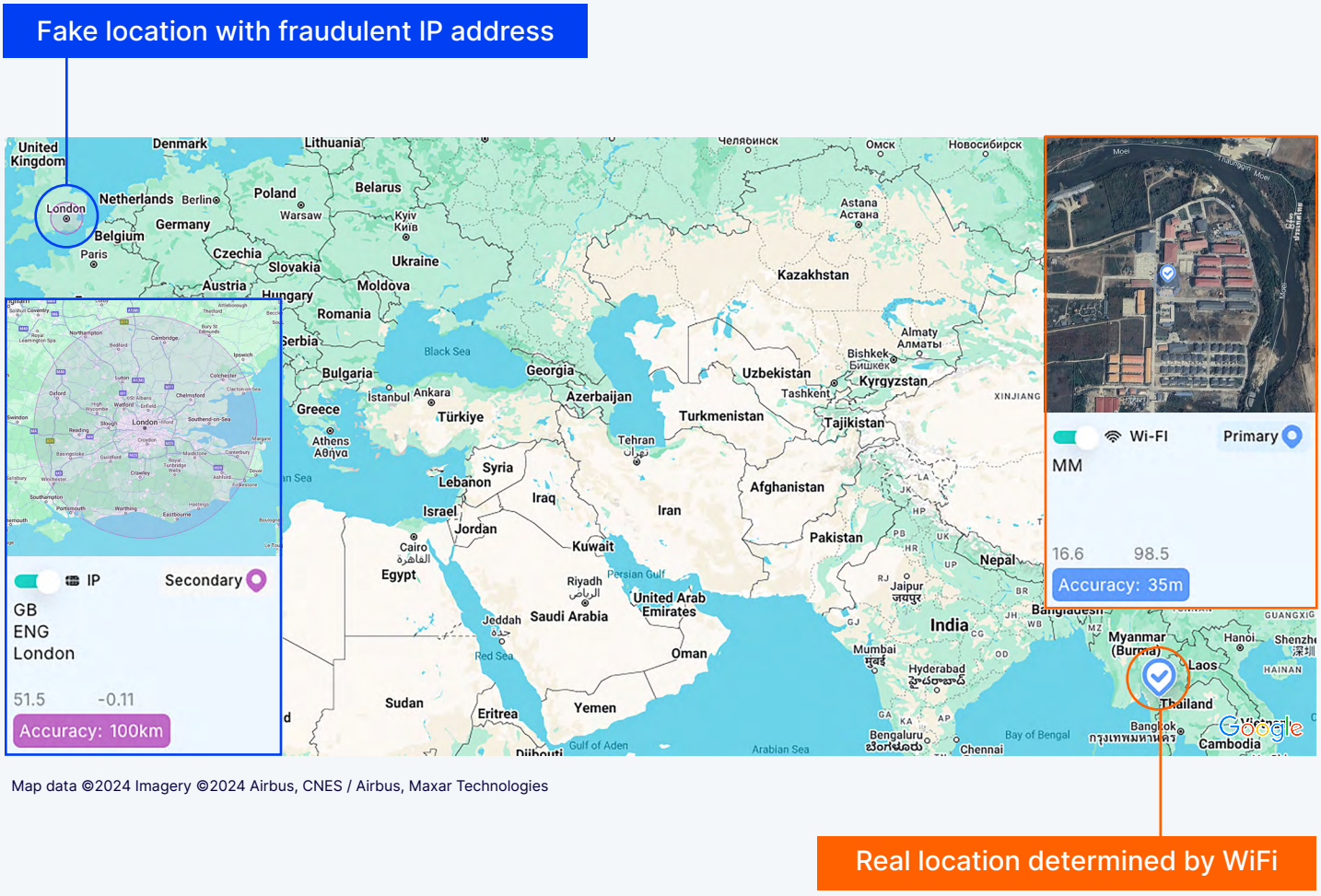
[8] Clara Fong and Abigail McGowan. How Myanmar Became a Global Center for Cyber Scams. Council on Foreign Relations. May 31, 2024
[9] The On-chain Footprint of Southeast Asia's 'Pig Butchering' Compounds: Human Trafficking, Ransoms, and Hundreds of Millions Scammed. Chainalysis. February 24, 2024
[10] Memorandum for the Subcommittee on National Security, Illicit Finance, and International Financial Institutions Hearing: "Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry". House of Representatives Committee on Financial Services. September 13, 2024

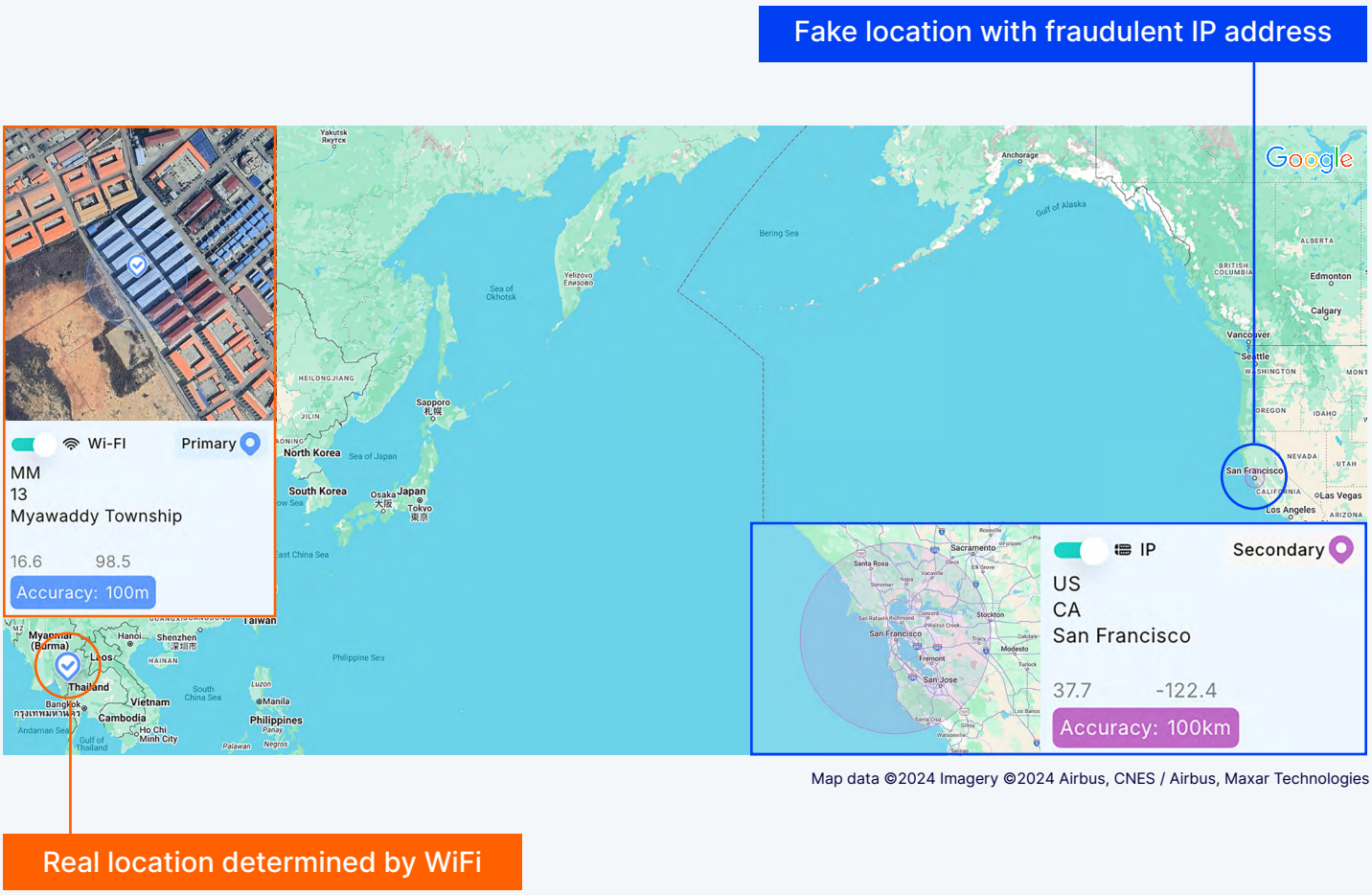
3 Extensive utilization of location obfuscation tools

Criminal organizations have an incentive to disguise their online behavior. While the most obvious way of doing so is through creating fake accounts, bad actors will also turn to location obfuscating tools to make it appear as though they are originating from less suspicious jurisdictions, often the same jurisdictions as their potential victims. While these tools include VPNs, there are other - often more sophisticated - tools, such as proxies, emulators, and the Onion Router, that enable online users to place their IP address in a geographic location of their choosing.

GeoComply's proprietary data suggests that location obfuscation is ubiquitous in jurisdictions associated with online scams. For example, nearly 85% of all observed digital interactions originating within Myanmar in 2023 were conducted with some form of location obfuscation tool.

Moreover, GeoComply has detected attempted transactions from known scam center locations in which criminal organizations have attempted to place their IP addresses in locations as varied as Southeast England, Central Kansas, and Downtown Bangkok.





Looking at IP addresses alone is insufficient to detect this obfuscation. To effectively root out illicit behavior, online platforms need to detect the presence of IP obfuscation tools, including - but not limited to - VPNs, while also aggregating supplemental location data points, including GPS, Wi-Fi, and Cell Tower information, to determine a user's true end location.

No one of these aforementioned steps is fully sufficient to detect and block fraudulent facilities, but looking at these signals holistically is a necessary step for online communication platforms to effectively detect, block, and report the locations of these fraud factories. The technology to halt and reverse the growth of these scams exist, but effectively isolating criminal fraudsters from our shared online communities requires powerful internet companies to act with moral clarity and embrace the power of data analysis.

Securing payment vectors

While improving location detection on communication channels is a necessary step to reducing criminals' ability to contact victims, payment channels also need to be cognizant of how embracing additional data signals can provide their users with further safeguards.

Within the crypto ecosystem, gangs use several different vectors to obtain payment, including fake crypto platforms[11], Bitcoin ATMs[12], and—critically—mainstream crypto platforms. Documents uncovered by Deutsche Welle show that the criminal enterprises operating these facilities explicitly instruct their slave laborers to use platforms like "Coinbase wallet."[13] It's critical for these mainstream crypto platforms to consider technical solutions that will safeguard their users and end their own inadvertent participation in this form of illicit finance.

When it comes to anti-money laundering and fraud-related regulations, crypto companies have a number of existing legal requirements codified in legislation such as the Bank Secrecy Act (BSA). The Financial Crime Enforcement Network (FinCEN), the government agency designed to ensure compliance with and enforce the BSA, has provided financial institutions (including crypto platforms) with several best practices for incorporating anti-pig butchering strategies into their BSA/AML frameworks.

In their 2023 guidance on pig butchering, FinCEN lists the following as a primary red flag:

"System monitoring and logs show that a customer's account is accessed repeatedly by unique IP addresses, device IDs, or geographies inconsistent with prior access patterns. Additionally, logins to a customer's online account at a [Virtual Asset Service Providers] come from a variety of different device IDs and names inconsistent with the customer's typical logins."[14]

The behavior FinCEN describes here indicates account sharing, the consensual disclosure of account credentials with another party (albeit, in this case, disclosure based on false pretenses). For example, a victim of pig butchering who has been manipulated into "investing" in a fraudulent scheme may create an account on a U.S. cryptocurrency exchange, using their own identifying information, load funds onto that account, and transfer their credentials to the scammer. **Assuming no location obfuscation was occurring,** this exchange of credentials to the overseas individual would likely violate a platform's velocity rule; the time and space between login attempts would mean it was physically impossible that the same user was accessing the account.

For this reason, and as we have discussed previously, gangs operating out of fraud factories will take steps to obfuscate their digital location identifiers, making them appear as though they are operating out of their victim's home country. The use of location obfuscation tools by criminals operating out of Southeast Asia renders this FinCEN red flag largely obsolete. Just as online communication platforms need to consider additional data sources to verify a user's true end location, crypto exchanges need to embrace more comprehensive geolocation tools to truly detect the movement of funds.

[11] Pig Butchering Crypto Scams Rising. Foodman CPAs & Advisors. September 25, 2024
[12] Ruiz, Rebecca. 'Nobody is immune': Don't fall for a Bitcoin ATM scam. Mashable. October 1, 2024
[13] Behind Asia's cyber slavery. Deutsche Welle. January 29, 2024
[14] FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering". Financial Crimes Enforcement Network. September 8, 2023

Additionally, fraudsters may try to directly take control of an end user's computer through a Remote Desktop Protocol (RDP). While there are legitimate reasons for turning control of one's computer over to a third party, such as legitimate tech support, turning control over for the purpose of receiving assistance with a crypto, or other financial transaction, is an immediate red flag. Even if a device appears to be in an expected location, remote access will be indicative that a true transaction beneficiary may not be the account holder. Looking at device intelligence indicators, such as mouse movements and running background applications, can help online financial platforms and cryptocurrency service providers detect RDP. Together, geolocation tools and remote desktop detection can strengthen a financial institution's defenses against pig butchering.

Staying ahead of the next scam

Pig butchering is a unique challenge. Not only does this form of fraud represent a unique threat to Americans' savings, and therefore, the country's broader financial stability, but the role pig butchering plays in funneling money into conflict zones, as well as inducing demand for human trafficking, means it constitutes a broader threat to global security. For the online platforms that are exploited by pig butchering gangs, incorporating additional data analytics into their security processes can be a small step with a massive positive impact for both themselves and society.

While pig butchering may not be a dominant scam typology in the long run, criminals are smart and resourceful. Their current behaviors demonstrate how lucrative it can be to use trafficked labor and online platforms for criminal gains. Ultimately, scams, fraud, and cybercrime may evolve, but without technical intervention, many of the same illicit behaviors may persist.

Only through an embrace of more advanced technical solutions can financial institutions and online communication platforms create effective countermeasures to this technology-enabled fraud epidemic.

GeoComply