Residential Proxies: What They Are and How They Affect Ad Fraud

Residential proxies are a tool for enhancing privacy and anonymity by masking their IP address to protect their digital identity.

Their use is widespread. Bright Data, a residential proxy service provider, boasts over 72 million unique residential IP addresses available in their IP pool.

But this functionality makes them attractive for abuse, such as ad fraud, where bad actors manipulate their trustworthiness to disguise traffic origin.

What is the extent of misuse? An IP address is a unique identifier assigned to each device on the Internet. Their misuse exploits this digital identity feature, allowing fraud activity concealment behind innocent-looking residential IP addresses. According to Arkose Labs, one in every five login attempts is an attempted account takeover (ATO).

This article covers residential proxies, how criminals abuse the proxy pool, and how businesses can protect themselves.

What are residential proxies?

Residential proxies are IP addresses leased from a residential internet service provider (ISP). They show up online as a standard home IP.

The primary function of residential proxies is to allow users to browse the internet anonymously, access geo-restricted content, or perform data collection without detection or reprisal.

This facade is useful for legitimate scenarios where privacy is paramount, such as journalists safeguarding sources or marketers conducting ad verification.

However, residential proxies enable bad actors to operate undetected to conduct questionable practices like web scraping, social media automation, and creating fraudulent ad results.

Are residential proxies legal?

Residential proxies are legal for legitimate uses such as privacy protection, market research, and content localization testing. Their legality hinges on consent and transparency. Businesses must use the proxies without breaching terms of service or privacy laws.

Ad fraud (generating fake clicks or impressions) is illegal and constitutes a misuse of residential proxies. These actions exploit paid advertising mechanisms, leading to financial loss through distorted analytics.

While residential proxies are legal, their application must not cross into misuse and criminality.

How do residential proxies work, and how do they impact ad fraud?

Residential proxy service traffic flow begins when the user's request routes through the ISP’s residential proxy server. The server forwards the request to the target website. Once the website responds, the data passes back through the residential proxy service to the user. This process cloaks the user's original IP address, substituting one that appears to originate from a typical home internet connection.

Some websites and online services have geo-restrictions on specific content or have defenses against automated bot detection systems. These sites are more likely to permit interactions from residential Ips without immediate blocking or blacklisting.

Bad actors use residential proxies to generate seemingly legitimate high-quality traffic, clicks, or impressions, making it difficult for ad networks and detection systems to differentiate from authentic user activity. This can result in a loss of credibility in the advertising ecosystem and a significant drain of resources, with businesses losing millions of dollars to ad fraud every year.

The different types of residential proxies

There are several types of residential proxy service, each with features serving unique purposes.

- **Shared ISP proxies:** Multiple users share residential IPs, making tracing and pinpointing fraudulent activities harder.
- **Rotating proxies:** Proxy rotation IPs for each request mimic genuine user behavior, evading algorithms designed to track IP use in ad fraud.

- **Dedicated residential proxies:** Individual users have unique IPs to exploit for ad fraud by maintaining a consistent, trusted online presence.
- **Mobile residential proxies:** IP addresses derived from mobile devices make them a prime target for abuse in less-monitored mobile ad platforms.
- **Static residential proxies:** A single unchanging IP is ideal for prolonged fraudulent campaigns.

Examples of residential proxy exploitation in ad fraud

Residential proxies have legitimate use cases — but bad actors use them for fraudulent techniques.

Web scraping and data harvesting

Web scraping uses automated scripts to extract website data, often for valid purposes like market research or price comparison. However, residential proxies can hide their origin, simulating diverse, legitimate user activities from various locations.

This technique produces fraudulent ad performance data collection and placement patterns. Consequently, artificially inflated ad traffic and concurrent impressions cause advertisers to pay for bot-generated views or clicks, not genuine customer engagement.

Market research

Residential proxies enable companies to access content and web data collection from various regions anonymously, simulating local users. This helps in competitor analysis, understanding market trends, and testing ad localization.

Fraudsters use this tool unethically to distort market research for competitive gain. They might use proxies from a residential proxy network to repeatedly visit competitor sites undetected, inflating traffic web data and skewing analytics.

Additionally, proxies can enable large-scale scraping of pricing, strategies, or product details, used to undercut prices or copy strategies, unfairly tilting the competitive landscape.

SEO monitoring and manipulation

Residential proxy network misuse can disrupt SEO by manipulating SERPs with fake clicks or queries to boost a website's popularity and ranking artificially. Posting backlinks across the internet under varied residential IPs falsely suggests widespread endorsement.

Additionally, proxies can facilitate negative concurrent SEO attacks, generating spammy links to harm competitors' reputations and rankings.

E-commerce actions

Price comparison manipulation, where bots scrape pricing and inventory data for unfair advantages, disrupts market equilibrium. Cart hoarding, manipulating inventory, and inflating prices can generate false demand.

Flash sales are abused by bypassing purchase limits, enabling bulk buying for resale at inflated prices to the detriment of genuine customers and brand reputation. Additionally, automated purchasing bots buy up high-demand items, outperforming real customers and eroding trust in the e-commerce platform.

Ad verification

Fraudulent traffic is masked by disguising web traffic origins, artificially inflating ad metrics through simulated clicks from various locations. Geo-targeting evasion occurs as proxies bypass ad restrictions, leading to ads reaching unintended audiences and misusing advertising budgets.

Ad cloaking involves hiding malicious content, displaying legitimate ads to verifiers while showing different content to others. Viewability fraud is perpetrated by creating fake ad impressions and clicks, blurring the line between real and fraudulent traffic.

Combating residential proxy misuse: What businesses should consider

Integrating Digital Element's IP intelligence and geolocation solutions enhances residential proxy provider detection while ensuring cybersecurity and compliance.

Enhanced security measures against proxy abuse

Machine learning systems can identify proxy service use by analyzing traffic patterns, IP reputation, and user behavior anomalies. IP blacklisting and whitelisting, coupled with rate limiting, manage traffic with IP blocks for known proxy IPs and limiting request frequencies to thwart automated tool overuse.

CAPTCHA challenges help distinguish between human users and scripts, while geolocation analysis checks for discrepancies between claimed locations and IP geolocations.

Robust multi-factor authentication strengthens account security, and continuous security audits ensure up-to-date defenses against evolving proxy service tactics. Additionally, educating employees on proxy usage, risks, and strategies, along with collaborating and sharing intelligence with industry peers, further bolsters a comprehensive approach against proxy abuse.

The role of legal compliance

Companies build secure relationships and maintain user trust by following data privacy laws like GDPR and CCPA.

A balanced approach prevents overreach, such as excessive proxy blocking that denies access to legitimate users. Ethical practices promote fair competition in sectors like e-commerce and digital advertising and discourage proxy misuse for unfair advantage.

Companies committed to ethical practices and compliance standards generally enjoy a better reputation and a significant market advantage.

Partnering with experts

Digital Element's advanced IP intelligence and geolocation solutions play a crucial role in detecting and combating misuse by a residential proxy provider.

Our accurate IP geolocation capabilities help identify traffic source discrepancies. This includes situations where a user's claimed location doesn't align with their IP address. With Digital Element, you can discern whether an IP address originates from a residential proxy network, VPN, or data center, enabling the filtering out of potentially fraudulent traffic.

These technologies also reduce ad fraud by verifying that ads display to the intended audience and not bots or users behind ISP proxies. Integrating IP intelligence into broader security systems enables monitoring unusual patterns, such as unexpected spikes in traffic from specific regions or IP ranges.

Our solutions also aid in compliance and risk management, reducing the likelihood of inadvertently engaging in or falling victim to fraud.

How to detect and block fraudulent residential proxies

A multifaceted approach combines various strategies and technologies, including:

Behavioral analysis

Detecting proxy misuse entails identifying behavior patterns atypical for genuine human users.

One indicator is a rapid sequence of actions, such as clicking links or filling out forms at inhuman speeds. Repetitive tasks, like regularly visiting the same pages or clicking on ads, also point to automated processes rather than human interaction.

Atypical geographical access occurs when a user appears to access digital assets from multiple locations within a short timeframe, suggesting proxies to mask real locations.

Additionally, irregular browsing patterns, such as directly accessing deep links without going through the home page, and high bounce rates paired with concurrent short session durations, often indicate bot activities like content scraping.

Specialized tools and methodologies are essential for implementation. Analytics tools like Google Analytics monitor traffic patterns and can set up anomaly alerts. Specialized anti-fraud software can detect bots and analyze behavioral patterns. Further, integrating behavioral biometrics, such as analyzing mouse movements, typing rhythms, and swipe patterns, adds another layer of analysis.

Machine learning and AI uncover complex patterns that might not be immediately apparent. User journey analysis, which benchmarks typical user paths, helps distinguish automated behavior from genuine user actions. Real-time monitoring is crucial in dynamic environments like e-commerce platforms or online advertising, where user behavior changes rapidly.

Advanced IP analysis

Detecting proxy usage involves a thorough examination of IP addresses across various aspects. Maintaining and regularly updating a database of known proxy IP addresses is crucial.

You can assess the reputation of an IP address based on historical web data and flags for proxy misuse. The allocation patterns of the IP addresses also provide insights; residential IPs are generally more legitimate, while data center IPs often suggest ISP proxies.

Several use cases are instrumental in IP analysis:

- Geolocation analysis helps assess the geographical origin of an IP address, uncovering discrepancies between the user-reported locations and actual access points.
- Autonomous system number (ASN) lookup is valuable in identifying the network from which the IP originates.
- Analyzing historical web data, including an IP's involvement in security incidents, helps evaluate the risk.
- Observing an IP’s traffic volume and patterns can indicate proxy automated processes.

Third-party proxy detection services

Digital Element's advanced proxy detection capabilities combine real-time analysis with a comprehensive IP address database, offering businesses a powerful tool in identifying and blocking suspicious IP traffic.

Our extensive databases include information on data center proxies, VPNs, and anonymizing services, enabling quick identification of potentially harmful traffic. Advanced detection algorithms analyze IP addresses in real time, identifying patterns that suggest proxy usage and helping to pinpoint new and evolving proxy methods.

These services also provide accurate geolocation data, which is crucial for businesses that deliver location-specific content and advertisements. This accuracy enhances user experience and ensures compliance with content licensing and privacy regulations.

Furthermore, Digital Element’s solutions improve overall digital security, preventing fraud and protecting against data breaches. By integrating these capabilities, businesses can effectively manage and mitigate the risks associated with proxy misuse, ensuring a secure and compliant digital environment.

Network fingerprinting

Network fingerprinting is a detailed technique for identifying devices through unique network characteristics.

Unlike standard IP analysis of geolocation and IP type, network fingerprinting delves into TCP/IP stack configurations, operating systems, browsers, and specific network settings. It examines packet structures and communication patterns to create a device fingerprint.

This method distinguishes real IP addresses from data center proxies by detecting network behavior anomalies. Proxies often alter network characteristics, but such modifications are identifiable through fingerprinting.

This technique is especially useful in spotting sophisticated data center proxies that mimic high-quality real user traffic, as it uncovers subtle network traffic markers.

Challenge-response tests

CAPTCHAs differentiate human users from automated traffic from data center proxies. They present challenges easily solved by humans but difficult for bots, like recognizing distorted text or identifying objects in images. This helps block or slow down bots performing social media scraping, spamming, or credential stuffing.

CAPTCHAs are effective in stopping basic automated attacks but have limitations. Advanced bots and AI can solve them with a high success rate, and some services use human labor to bypass these challenges. Additionally, complex CAPTCHAs can be inaccessible or frustrating to genuine users.

As technology evolves, balance CAPTCHA implementation with user experience. Less intrusive methods like reCAPTCHA or invisible CAPTCHAs help maintain security without adversely affecting user experience.

Better protect your digital landscape with Digital Element

Residential proxy usage in ad fraud presents significant concurrent risks, including skewed advertising metrics, wasted budgets, and compromised campaign integrity.

Advanced technologies offered by Digital Element have a high success rate in detecting such risks. Our sophisticated IP intelligence and geolocation solutions provide the necessary tools to discern genuine user interactions from those masked by data center proxies.

For more information on how Digital Element's solutions can safeguard your digital advertising efforts, visit us online.