One Step Closer to Fraud Prevention with WHOIS, IP, and DNS Intelligence

As of the third quarter of 2021, the FTC Consumer Sentinel Network received more than 1.6 million fraud complaints, amounting to a total of US$3.5 billion in losses.

WhoisXML API's WHOIS, IP, and DNS Intelligence can enrich fraud detection and prevention systems to help organizations minimize fraud cases and associated losses. How so exactly? This white paper looks at major types of fraud and the key questions that our data capabilities can help you answer.

You can also download additional fraud research materials compiled on our site with specific examples of our intelligence in action.

1. Content Abuse and Account Takeovers

About-Fraud defines an account takeover as "the unauthorized access of a user's account to steal identity credentials, execute a fraudulent transaction, or engage in varying types of abuse." This type of fraud can be accomplished in several ways, including subdomain takeover, DNS cache poisoning, DNS hijacking, and DNS tunneling.

Content abuse, another fraud type identified by About-Fraud, can also lead to account takeovers. Some examples of content abuse are spamming and phishing, website defacement, and other ways of posting content to abuse and deceive a company and its stakeholders. In these attacks, threat actors usually impersonate the organizations so their fake content would seem legitimate. They may employ attack vectors, such as cybersquatting domains, and attack methods like DNS spoofing and domain hijacking. WhoisXML API's domain and DNS intelligence can help monitor domains, subdomains, and DNS records to prevent cyber attacks that could lead to content abuse and account takeovers.

Notable Use Cases	Relevant Data Points
Detection of dangling DNS records	• When were the subdomain records last updated? • Are there unused subdomains? • Are there outdated DNS records?

Verification and checking of DNS configurations	• Do DNS records follow ideal settings, such as recommended time-to-live (TTL) and naming conventions? • Are DNS resolutions correct? • Have unauthorized changes been made to the DNS records?
Detection of cybersquatting and typosquatting domains and subdomains	• Are there recently added domains and subdomains that contain the company's name? • Are there recently added domains and subdomains that contain the names of company executives? • Are there look-alike domains registered in bulk in a given day, week, or month?
Domain monitoring	• What is the current status of your domain name? Does the status code provide protection against domain hijacking? • Have unauthorized changes been made to a domain's WHOIS record? • What is your registrar's contact information if you want to change status codes or report cases of unauthorized changes?

2. Social Engineering and Authorized Push Payment Fraud

Authorized push payment fraud refers to the process of manipulating a legitimate customer to make a payment to an account controlled by the fraudsters. About-Fraud identified several types of authorized push payment fraud, including romance and invoice scams. These scams are often accomplished through phishing, where fraudsters posing as company representatives demand payment from customers. Fraudsters can also hijack or poison the customers' DNS cache to redirect users to malicious web pages.

While attackers can accomplish authorized push payment fraud in several ways, WHOIS, IP, and DNS intelligence can help minimize risks of exposure.

Notable Use Cases	Relevant Data Points
Detection of cybersquatting domains and subdomains	• Are there recently added domains and subdomains that could be used to imitate the company in email communications? • Are there recently added domains and subdomains that contain the names of company executives? • Have look-alike domains been reported as malicious?
Email verification	• Are their messages sent to network users that are from disposable email domains? • Are their disposable email domains that contain your company name?

3. Card-Not-Present Fraud

According to this report, card-not-present (CNP) fraud is one of the most rampant types of e-commerce fraud, accounting for 10–13% of digital transactions from Q1 2020 to Q1 2021. CNP fraud costs e-commerce companies millions of dollars in chargeback fees, among other damages. As fraudsters take advantage of technology advancements to perform CNP fraud, organizations can fight back using combined intelligence sources. Here's how WhoisXML API can help.

Notable Use Cases	Relevant Data Points
Financial transaction verification	• Are the customer's recorded IP address, Internet service provider (ISP), and connection type the same at the moment of the transaction? • Is the customer's IP address malicious or located in a cybercrime hotspot at the time of the transaction? • Does the financial transaction originate from out of the region or offshore?
Ongoing customer monitoring	• Are transactions or activities suddenly originating from out-of-service areas? • Do any of the recent transactions come from a malicious IP address or cybercrime hotspot?

4. Promo Abuse

Promo abuse occurs when the terms of service (ToS) of promotional offers are exploited to avoid payments or obtain significant discounts. Companies offering digital products and services encounter this type of fraud in the form of freemium abuse, where users sign up for multiple free accounts to circumvent limitations and avoid upgrading to paid subscriptions. Preventing this kind of abuse can begin upon signup using WhoisXML API's email verification tools.

Notable Use Cases	Relevant Data Points
Email address validation	• Does the user's email address follow the correct syntax? • Does the email address have an existing mailbox and corresponding mail server? • Can the email address receive messages?
Detection of email address type	• Is the new user signing up using a disposable email address? • Did the new user type in a catch-all email address? • Did the new user sign up with a business email address?

5. Reseller Abuse and Counterfeiting

Different types of fraud, such as reseller abuse and counterfeiting, can also damage a company's brand reputation. WhoisXML API's WHOIS, IP, and DNS intelligence can strengthen security measures against these forms of abuse.

Notable Use Cases	Relevant Data Points
Detection of cybersquatting domains and subdomains	• Are there domains and subdomains that contain the company name? • Have look-alike domains and subdomains been reported as malicious? • What do the web pages hosted on the cybersquatting domains and subdomains look like? Do they resemble the official website of the imitated company?
Monitoring of resellers and possible counterfeiters	• Have domains sporting a reseller's or known counterfeiter's name and email address that seem to imitate a company been recently registered? • What do the reseller's domain resolutions look like? Are there web pages that hint at reseller abuse or counterfeiting? • Were changes made to the nameserver of a known cybersquatting domain?
Prevent trademark infringement and support Uniform Domain-Name Dispute-Resolution Policy (UDRP) complaints	• Do existing and newly added domains and subdomains seem to be imitating yours? • What content do these domains and subdomains host? Does the content indicate that cyber resources were added in bad faith? • When were these typosquatting domains and subdomains added?

6. Synthetic Identity Fraud

Synthetic identity fraud refers to the fabrication of a person or entity using the personally identifiable information (PII) of different people. In this type of fraud, the fraudster aims to make unsuspecting victims believe that the identity is real and convince them to engage in financial transactions with the made-up person or entity. Fraudsters can pose as suppliers, partners, customers, or any entity that can help them profit off malicious activities. WhoisXML API's domain, IP, and DNS intelligence can help create profiles and validate identities.

Notable Use Cases	Relevant Data Points
Supplier profile risk assessment	• What are the domain's registration details and have they been redacted? Do they match the details the third party provided? Were the same details used for malicious domains? • How is the supplier's website categorized? • Is the domain or IP address classified as malicious? Was the supplier's domain registered in a high-risk location? • Are the supplier's nameserver, ports, and Secure Sockets Layer (SSL) certificates configured correctly?
Customer identification and validation	• Is the customer's IP address located in a cybercrime hotspot? Was the customer's domain name registered in a high-risk location? Are any of your customers' domains and IP addresses flagged as malicious? • Does your customer's website details match those documented in DNS and WHOIS records? Does the website fall under dubious categories? • Which other domains share the customer's IP address? Are they part of a dedicated or shared infrastructure? Are they malicious?

About Us

WhoisXML API aggregates and delivers the most comprehensive domain, subdomain, IP, and DNS data repositories. Our intelligence is accessible via different consumption models, including APIs, data feeds, monitoring tools, and web-hosted reports. WhoisXML API has more than 50,000 satisfied customers from various sectors and industries, such as cybersecurity, marketing, law enforcement, e-commerce, financial services, and more. Visit whoisxmlapi.com for more information about our products and capabilities.