Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Amplify Anti-Fraud Efforts in the Financial Sector with Internet-Wide Visibility

Business Problem

While no one is immune to fraud, financial institutions, such as banks, credit card companies, and payment processors, are prime targets, as evidenced by a 149% increase in fraud attempts in 2021-125% higher than the global average across all sectors. Transaction fraud cases, account takeovers, impersonation, financial scams, and phishing continue to bombard financial companies and their clients left and right. These fraud types primarily use the Internet as a vehicle, and therein lies a major challenge—fraud fighters need to keep up with the ever-changing and constantly expanding amount of data in the digital space. As such, financial organizations need to equip anti-fraud strategies and solutions with Internet-related data that can detect, unmask, and ultimately deter fraudsters.

Data-Driven Solution

Fraud prevention strategies need to be intensified as digital financial transactions have become the norm. That can be done by leveraging high-fidelity data relevant to the world's Domain Name System (DNS), including domain, WHOIS, IP, and other Internet records. Finding the right data partner that can provide fresh and historical WHOIS and DNS data while offering flexible and scalable consumption models and enterprise-grade customer support is essential in the fight against fraud. Real-time access to these data sources is pertinent for the early detection and mitigation of suspicious transactions, while historical DNS data can shed light on the cyber resources fraudsters weaponize.

Notable Use Cases	Connected Data Points
Detect fraud at the transaction level	• Are the customer's recorded IP address, Internet service provider (ISP), and connection type the same at the moment of the transaction? Discrepancies in these critical records may suggest unauthorized transactions. • Is the customer's IP address malicious or located in a cybercrime hotspot during the transaction? If so, you may want to protect clients by employing additional identity verification methods. • Does the financial transaction originate from out of the region or offshore? Can account owners reasonably travel and perform transactions from their previous location to the current one? A significant distance within a short span of time in-between transactions could suggest card-not-present (CNP) fraud or similar scams not requiring the physical presence of the account holders or their cards.
Prevent authorized push payment fraud	• Are there disposable emails and recently added domains and subdomains that could be used to imitate the company in email communications? Clients might be quick to act on money transfer requests and payment demands from a similar-looking email address (e.g., customersupport@paypai[.]com). • Are there recently added domains and subdomains that contain the names of the company's executives? These resources could be used to imitate corporate leaders in malicious email communications, including those asking for payment. • Have any of the look-alike domains been reported as malicious? Their presence in malware engines and reports means they have been used in business email compromise (BEC) scams, phishing, or other malicious campaigns.
Uncover synthetic identity fraud	• Is the new client using a disposable email address (DEA)? While DEAs may help protect privacy, they can also hide sinister or made-up personalities. • Is the customer's IP address located in a cybercrime hotspot? Additional security measures, such as a more stringent identification verification process, may be required for clients in these areas. • Which other domains share the customer's IP address? Are they part of a dedicated or shared infrastructure? Are they malicious? Gleaning these insights from the client's connections can help uncover suspicious details regarding their identities.
Impede account takeovers	• Do you have dangling DNS records from unused subdomains or de-provisioned cloud instances? These could make the company vulnerable to subdomain takeover attacks, leading to account takeovers. • Are there recently added domains and subdomains that contain the company's name or its executives? Are there look-alike domains registered in bulk in a given day, week, or month? Cybersquatting domains can be used in phishing campaigns that aim to steal clients' credentials so threat actors can take over their accounts. • Have unauthorized changes been made to your WHOIS and DNS records? Monitoring domain statuses and DNS configurations can help prevent attackers from taking control of the company's infrastructure, thereby protecting user accounts and data as well.

> **Being able to analyze and examine user accounts and transactions in light of the domain and IP data provided by WhoisXML API has helped us detect suspicious activity. Many times, this had led to the discovery and prevention of fraudulent transactions that would have cost us and our customers a lot more. *We're* glad to partner with them in our fight against fraud.**

Head of Anti-Fraud and Credit Authorization Department
Commercial Bank

> **We found certain nameservers that were always used for a phishing campaign, having those in our rules enabled us to catch phishing sites before they affected our user base. WhoisXML API is a responsive and reliable provider of domain intelligence. Whenever there are issues, they are quick to respond and resolve them. Working with them is smooth and straightforward.**

Christine Bejerasco, Senior Analyst
F-Secure Labs

Finding Your Own DNS Data (FYODD) Doesn't Let You Scale

Delivering a real-time and uninterrupted satellite view of the world's DNS is our core business. The WhoisXML API data engine is built and frequently upgraded to offer you the most complete, updated, and unique Internet intelligence footprints. We aim to contribute to our clients' competitive edge at every step and give back months or years of development cycle time to your most pressing and mission-critical projects and deployments.

How the WXA Data Engine Is Ready to Add to Your Success Today

1. Collection	2. Unification	3. Maintenance	4. Delivery	5. Innovation
• Internet-wide data sensing and crawling since 2010 • Legal agreements with major data aggregators • Large and growing network of data exchange partners	• Consistent data parsing of multiple data points across formats • Resolving incomplete, conflicting, and inaccurate records	• Addition of new and historical domains, subdomains, and IP and DNS records • Daily updating of millions of WHOIS, DNS, IP, and other records	• Batch feeds and APIs with complete documentation • Different support and customer success tiers • Streaming of domain and DNS data in real-time • Enterprise-grade IT infrastructure	• Ongoing improvement of data coverage, freshness, and accessibility • New features, product iterations, and solutions driven by market demand

Our Enterprise Value Proposition

Our intelligence is available through customized enterprise packages and product suites with multi-year contracts, flexible licensing models, nonrestrictive data access, and dedicated account and customer success teams. Contact us for more information.

Diamond: Includes all products listed below with Premium SLA
Gold: Pick 2 of each Tier, includes Gold SLA
Silver: Pick 1 of each Tier, includes Silver SLA
Starter: Pick 1 Tier-1 product, 1 Tier-2 product

Tier	Product	Update Frequency
P	Real-time & Historic Whois Streaming	Real-time Stream, Daily & Quarterly Feed, Real-time API Lookups
P	Real-time & Historic Passive DNS Coverage	Daily + Weekly Feed, Real-time API Lookups
P	Enterprise & Threat Intelligence APIs	Enterprise APIs T5 & Threat Intelligence APIs (1M CPM)
1	Real-time WHOIS Data Coverage	Daily & Quarterly Feed, Real-time API
1	Real-time DNS Coverage	Weekly Feeds, Real-time API
1	IP Geolocation & Netblocks Data Coverage	Daily Feeds
1	Website Contacts & Categorization Feed	Daily Feed
2	Subdomains Database Feed	Daily Feed
2	IP Netblocks (IPv4 + IPv6)	Daily Feed
2	IP Geolocation Database	Daily Feed
2	Typosquatting Data Feed (Enriched)	Daily Feed
2	Disposable Email Domains Feed	Daily Feed
2	MAC Address Database Feed	Daily Feed

About Us

WhoisXML API aggregates and delivers comprehensive domain, IP, DNS, and subdomain data repositories. WhoisXML API has more than 52,000 satisfied customers from various sectors and industries, such as cybersecurity, marketing, law enforcement, e-commerce, financial services, and more. Visit whoisxmlapi.com or contact us for more information about our products and capabilities.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence