The Domain Research Suite That Aids Financial Fraud Investigations

Posted on October 24, 2019

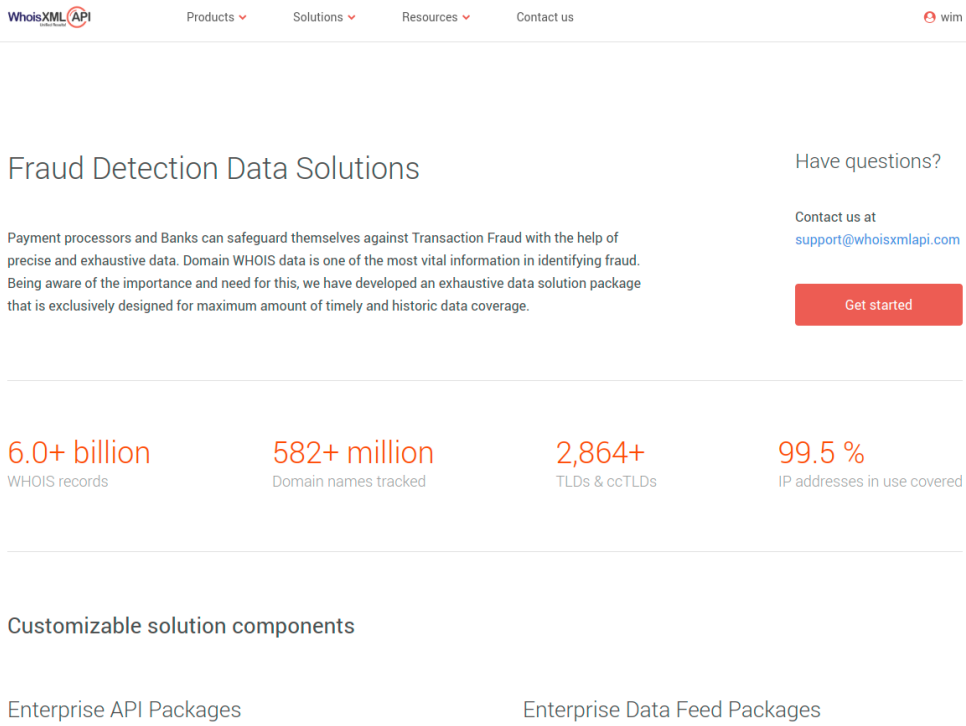
Cryptocurrency Exchanges Go Unregulated

Bitsane, a cryptocurrency exchange based in Ireland, vanished in the June of 2019. Its founders took with them the crypto deposits of 246,000 users. The platform traded an average of $7 million each day.

Worldwide, fraudsters stole nearly $1.5 billion's worth of cryptocurrencies in the first two months of 2018 alone. It's estimated that since then, criminals have made off with an average of $9 million a day.

So how can law enforcement authorities, legitimate financial institutions, and even individuals know whether a cryptocurrency exchange is planning to steal customer investments?

WHOISXMLAPI.com's Domain Research Suite can reveal indicators that financial institutions like cryptocurrency exchanges may be committing fraud.



WHOISXMLAPI.com researchers decided to apply a combination of traditional online investigation with WHOISXMLAPI.com's Domain Research Suite to determine whether a current cryptocurrency exchange had intentions to defraud customers. Though perhaps not attributable to luck so much as a high probability of discovery in today's crypto Wild West, WHOISXMLAPI.com researchers did discover an operational exchange that was already collecting customer complaints.

Though we can't name the company we investigated, we will show you the tools and publicly available online databases we used to delve beneath the surface hype of the Exchange.

Financial Fraud – Consumers Cheated

Ripoff Report is one of the most popular repositories on the Internet for filing "complaints, reviews,

scams, lawsuits, and frauds. It happens to have categories for Bitcoin Fraud and BTC Fraud, among other listings. It's in these categories that we discovered complaints against what we'll call ExchangeXYZ (not its real name). Googling "ExchangeXYZ Reviews" revealed even more complaints over the past seven months from customers (with attendant entries from individuals promoting services to reclaim lost funds).

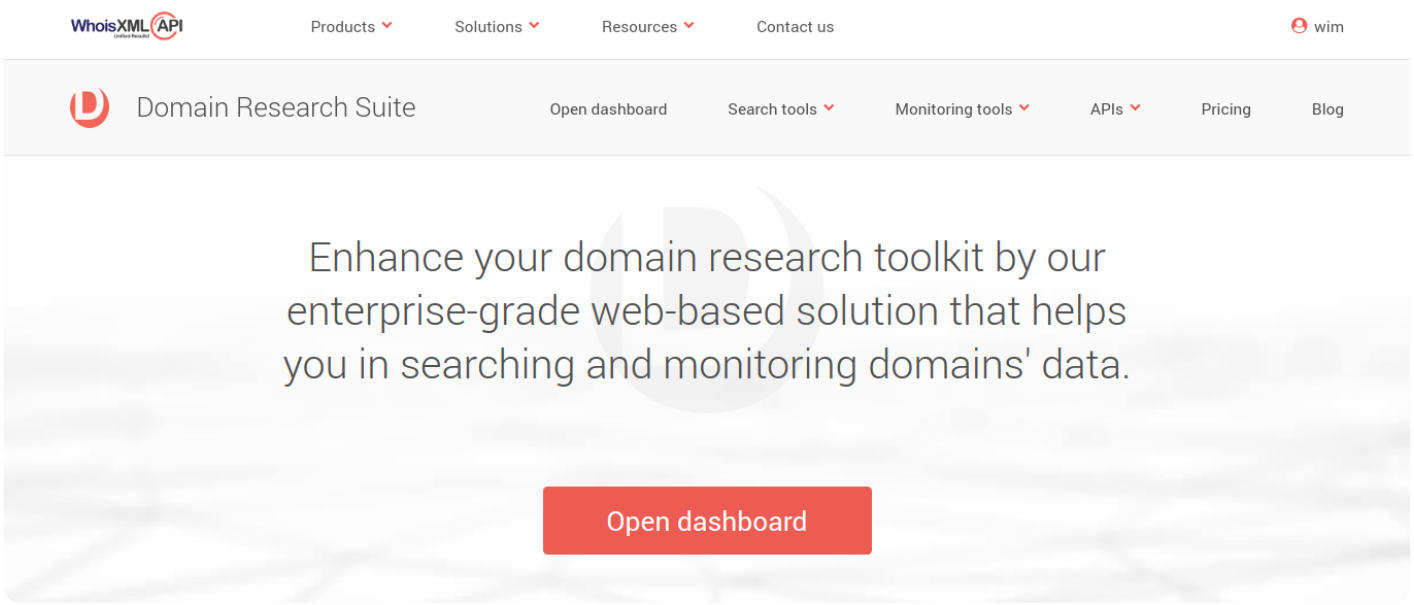
Typical complaints we took as red flags were much like this one:

"… they have held my bitcoin for over 7 months even after going through the verification process[,] they refuse to allow my bitcoin to be sent to my whitelisted wallet … [ExchangeXYZ] has given me every excuse imaginable … [It is] how they are holding value in their Exchange… [ExchangeXYZ] wants to operate in the USA[,] but with my experience I would never recommend putting any crypto currency in this exchange as you will not get it back…"

A look at ExchangeXYZ's website revealed no contact details: addresses, phone numbers, or even a chat line. However, there are about a half dozen email addresses that have to do with PR relations, product information, coin exchange information, etc. The only means of customer support is through a form on the website. Several of the complainants noted that any responses they received by using the form were clearly from bots, without any human intervention.

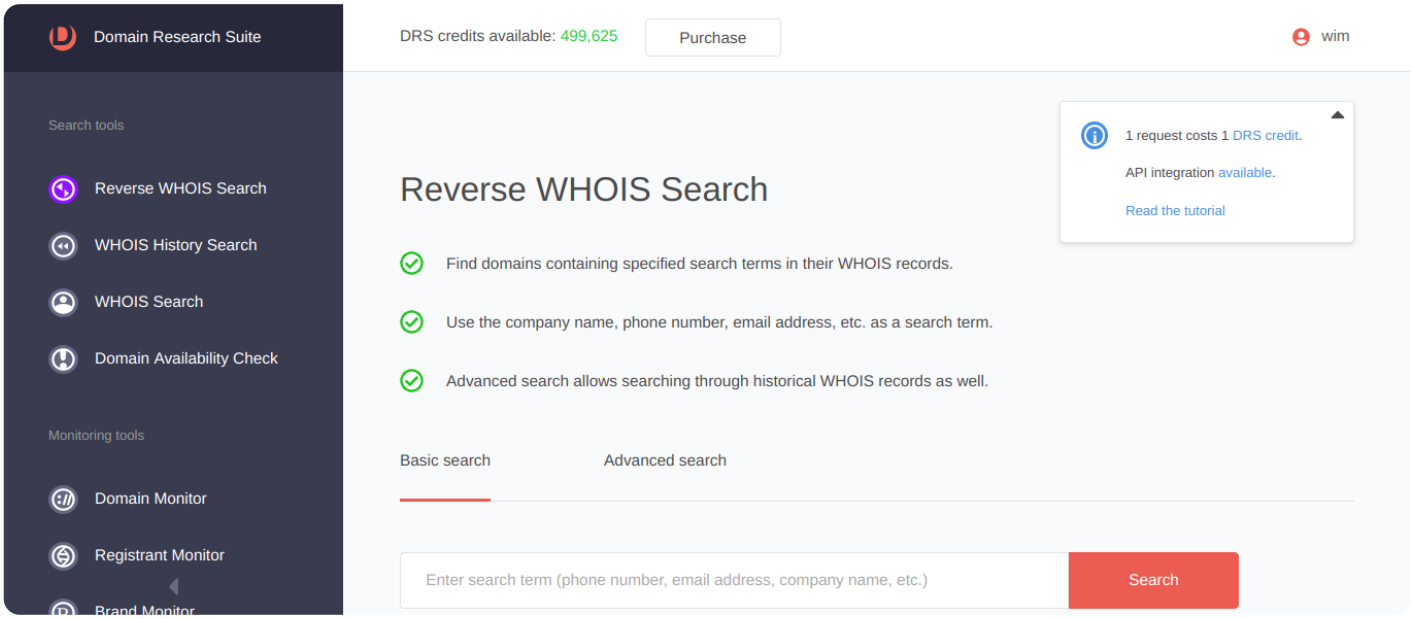
Using the Domain Research Suite to Investigate

The WHOISXMLAPI.com Domain Research Suite revealed that the registrar for the company's website was a registration service based in Denver, Colorado.

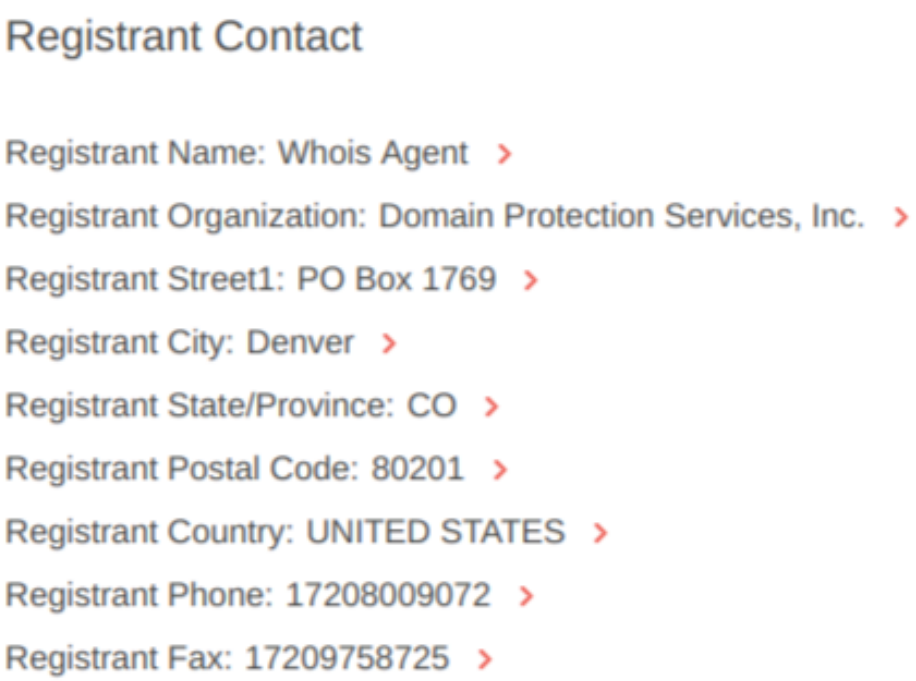


The Domain Research Suite sports a dashboard with easy-to-use tools that excavate the backgrounds of websites. The tools include:

- Reverse WHOIS Search – use company and contact information to learn about domains
- WHOIS History Search – find out about the ownership history of a domain
- WHOIS Search – learn about the current owner and administrator of a domain



The WHOIS Search delivers data about the owner of a domain, the owner's address, as well as the administrator and similar contact information. In the event of a WHOIS Search on ExchangeXYZ, the location of the registrar would initially lead a consumer to believing the company is based in the U.S. At the very least, as we've seen from the representative customer complaint above, ExchangeXYZ is servicing consumers in the U.S.



Registrant Contact

Registrant Name: Whois Agent
Registrant Organization: Domain Protection Services, Inc.
Registrant Street1: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: UNITED STATES
Registrant Phone: 17208009072
Registrant Fax: 17209758725

According to the WHOIS records of the top ten cryptocurrency exchanges, four of those either used agents to protect their identities or they edited contact information to block prying eyes. So it is not extraordinary that

The U.S. Securities and Exchange Commission (SEC) cites that "…if a platform offers trading of digital assets that are securities and operates as an "exchange," as defined by the federal securities laws, then the platform must register with the SEC as a national securities exchange or be exempt from registration." A search of the SEC's EDGAR database of registered corporations showed no record of ExchangeXYZ. Nowhere on the website does it indicate it has either registered with the SEC or been exempt by the regulatory body. In other words, the SEC could not protect American consumers who traded on the suspect cryptocurrency platform.

The New York State Attorney General also believes that ExchangeXYZ and others are indeed servicing customers in the United States, including New York State. In 2018, the New York State Attorney General released a voluntary survey for 13 cryptocurrency Exchanges to complete about

their operations. All but four Exchanges returned the surveys. ExchangeXYZ was one of the four that refused to respond. The Attorney General's office concluded in its September 2018 report that as their report details, "many virtual currency platforms lack the necessary policies and procedures to ensure fairness, integrity, and security of their exchanges." The Attorney General's report detailed how some of the platforms practice overlapping lines of business that present "serious conflicts of interest". Some, the report observed, traded for their own account on their own venues.

Indeed, Bitwise Asset Management, a cryptocurrency asset advisory and management firm, cited in a report that upwards of 95% of cryptocurrency trading originated from suspect sources. Research firms Crypto Integrity and The TIE concluded that 88% and 75% of reported exchange trading data were suspicious, according to the The Wall Street Journal (WSJ). The WSJ report pointed out that "the unregulated exchanges are inflating trading volume to get a higher ranking on data services like CoinMarketCap and leverage that ranking to attract listing fees."

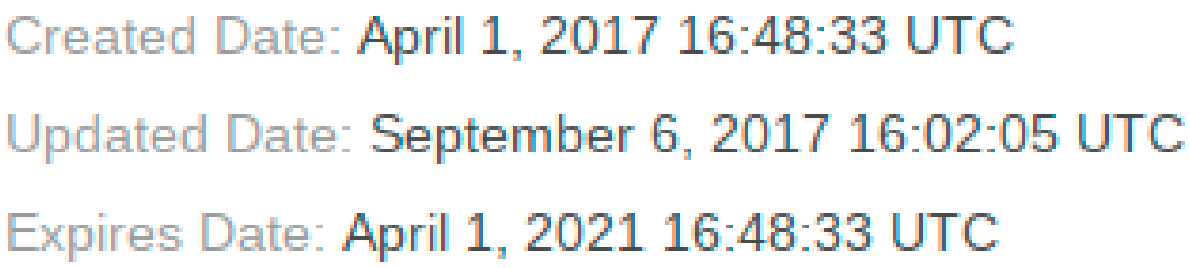
In light of its own findings, the New York Attorney General's office has since formally referred three of the Exchanges to the New York State Financial Services department to investigate whether the Exchanges are operating illegally in New York State. One of the three is ExchangeXYZ.

So why is it that ExchangeXYZ can ignore some of the most powerful financial regulatory agencies in the world? A peek at its domain history may give some clues.

A Look at the WHOIS History of ExchangeXYZ

The WHOIS History shows the domain name was registered in China on April 1, 2017. This occurred during China's own cryptocurrency Wild West when Mainland Chinese residents were desperate to move their money offshore through cryptocurrency exchanges. The exchanges at the time afforded customers an unregulated way to realize foreign exchange beyond the limits set by the government. The timing also suggests how ExchangeXYZ got so big so quickly. But the Chinese government effectively outlawed cryptocurrency exchanges later in 2017. ExchangeXYZ's founders had started the business in China at the worst possible time, it seemed.

So it chose to go West.



WHOIS HISTORY API (on October 2, 2017)

Registrant Contact

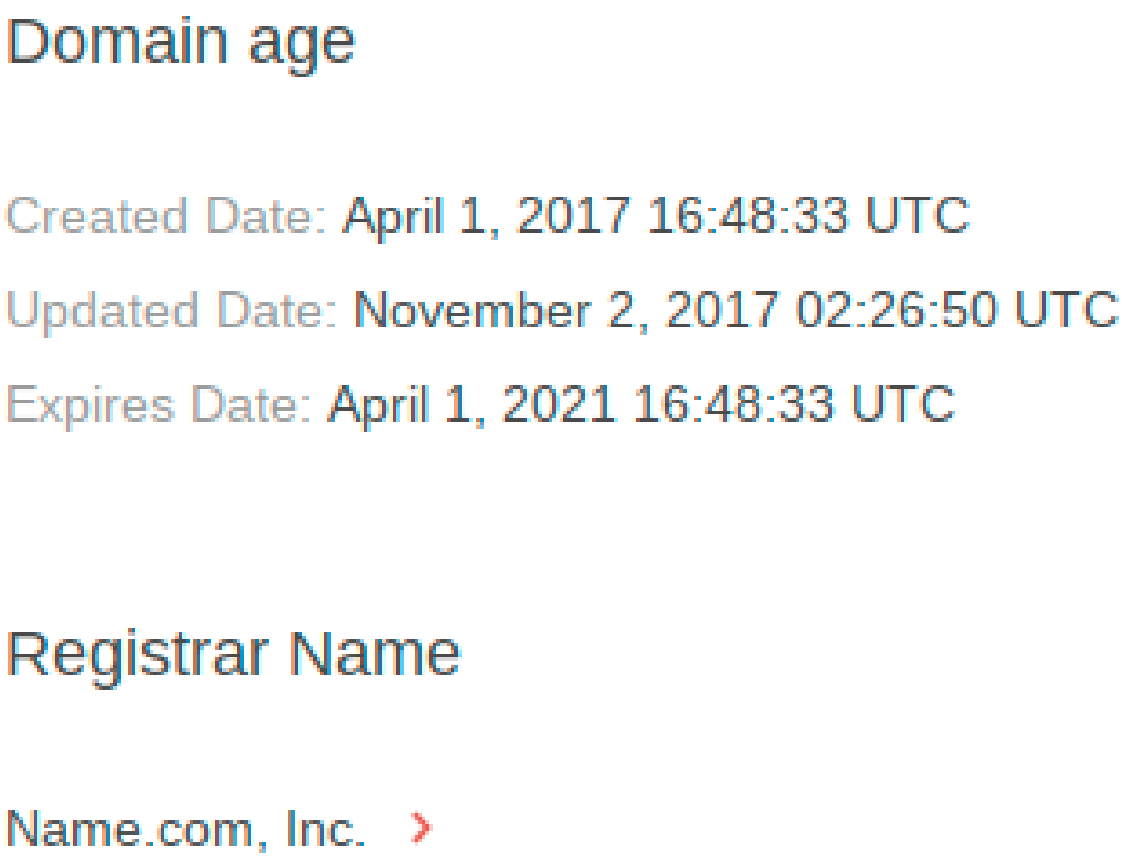
Registrant Name: [redacted] chen
Registrant Organization: Shanghai [redacted] Enterprise Management Consulting Co. Ltd.
Registrant Street: Shanghai city Chongming County Town East River [redacted] (Shanghai City Economic Development Zone)
Registrant City: Shanghai
Registrant State/Province: Shanghai
Registrant Postal Code: 200000
Registrant Country: CHINA
Registrant Email: [redacted]
Registrant Phone: 86[redacted]

Administrative Contact

Administrative Name: guangyin chen
Administrative Organization: Shanghai Bijie Enterprise Management Consulting Co. Ltd.
Administrative Street: Shanghai city Chongming County Town East River [redacted] (Shanghai City Economic Development Zone)
Administrative City: Shanghai
Administrative State/Province: Shanghai
Administrative Postal Code: 200000
Administrative Country: CHINA
Administrative Email: [redacted]
Administrative Phone: 8613761038500

WHOIS HISTORY API (on October 2, 2017)

In December 2017, ExchangeXYZ chose to use a professional domain service firm based in the United States to protect the national origin of its domain.



WHOIS HISTORY API (on December 18, 2017)

Note that the Created and Expired dates of the October 2, 2017 and December 18, 2017 coincide. On December 18, 2017, the domain creator chose to mask the origin of the domain with a U.S.-based service provider. The time frame fits in with the operation wanting to hide its China-based domain registration, more likely from the authorities on Mainland China and, perhaps, even from the Japanese authorities.

So the question remains: is it common practice for cryptocurrency exchanges to hide their provenance? The answer is “no”. Of the ten most popular exchanges, six have made their

ownership history explicit in the WHOIS historical record. Two explicitly state their records have been “edited”, while a truly U.S.-based one has used a Panama-based administrator to maintain its current record.

Why, then, would ExchangeXYZ choose to hide its origins from occasional viewers?

Shell Companies, Shell Game

ExchangeXYZ moved its operations to Malta during the spring of 2018, according to its Wikipedia entry. Malta is known best for three things: the 1941 film *The Maltese Falcon*; its government-sanctioned sales of European Union passports to Russian oligarchs; and its reputation as an offshore banking financial center. Malta’s lax financial regulatory environment is a magnet for companies that wish to escape scrutiny.

However, just because a business is registered in Malta, it isn’t necessarily looking to escape the regulations of other countries.

Perhaps an investment entity is offering local services. A search on Google, however, indicated no website based in the island-nation related to the company, and no business activities to speak of. Further, a search with WHOIS API on the several Maltese business names of ExchangeXYZ did not reveal any domains.

As the noted financial fraud investigator Travis Birch observes:

“These days, it makes sense for almost every business to have a web presence, even if they aren’t dealing directly with end customers. This could be an Alibaba shop, a Yellow Pages listing, a proprietary website, or anything that states the company’s line of business. A lack of effort to promote itself suggests that the company may not want to be known.”

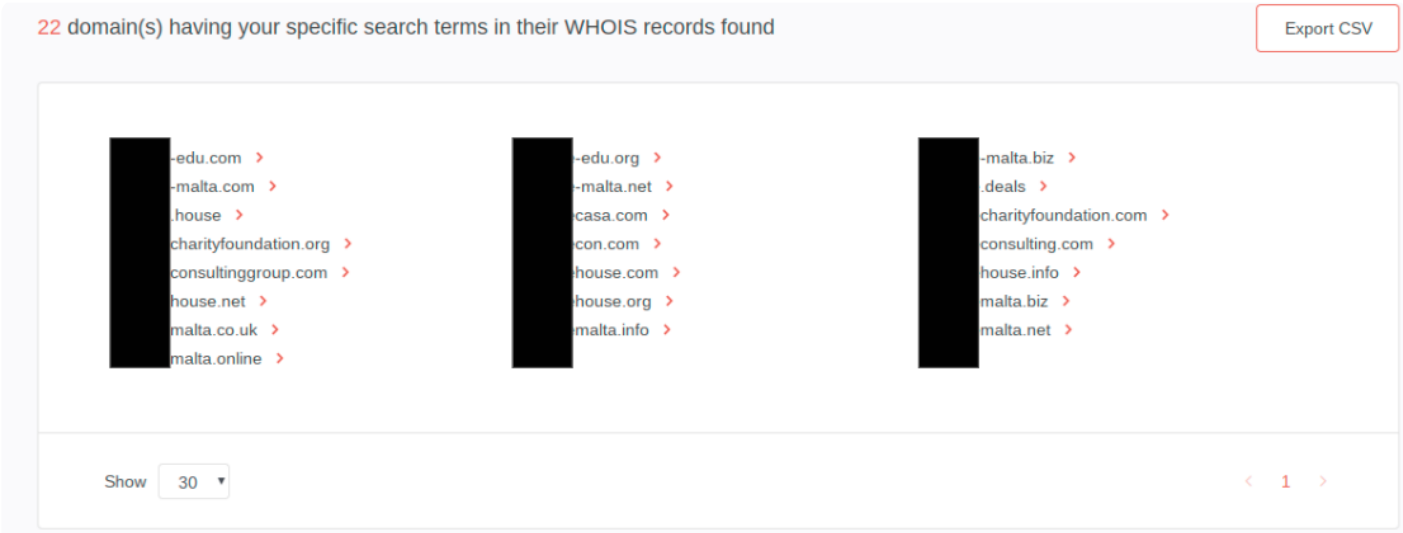
Further, a search on the address of the two Maltese addresses at which ExchangeXYZ entities are

registered reveal dozens of companies at the same street address revealed as shell companies in The Offshore Leaks Database. The Database houses the Panama Papers as an indexed repository of the business entities in offshore locations revealed in 2015 as shell companies.

75 LIMITED	06-NOV-2006	Malta	Malta	Paradise Papers - Malta corporate registry
ASSOCIATED FREEZERS LIMITED (D 75)	24-JUN-1966	Malta	Malta	Paradise Papers - Malta corporate registry
CHAPTER 75 LTD.	07-APR-2014	Malta	Malta	Paradise Papers - Malta corporate registry
MERCHANT STREET HOLDING LIMITED	27-AUG-2014	Malta	Malta	Paradise Papers - Malta corporate registry
MERCHANT STREET LIMITED	27-AUG-2014	Malta	Malta	Paradise Papers - Malta corporate registry
25 WATT STREET LIMITED	12-SEP-2014	Malta	Malta	Paradise Papers - Malta corporate registry
JK 75 LTD	09-FEB-2015	Malta	Malta	Paradise Papers - Malta corporate registry
BAY STREET OPERATIONS LIMITED	23-FEB-2015	Malta	Malta	Paradise Papers - Malta corporate registry
SOUTH STREET PROPERTIES LIMITED	20-JAN-2016	Malta	Malta	Paradise Papers - Malta corporate registry
MAIN STREET LIMITED	15-FEB-2016	Malta	Malta	Paradise Papers - Malta corporate registry
MOLL STREET LIMITED	22-FEB-2016	Malta	Malta	Paradise Papers - Malta corporate registry
Baker Street Patisseries Limited	07-APR-2016	Malta	Malta	Paradise Papers - Malta corporate registry
197 MAIN STREET LIMITED	23-MAY-2016	Malta	Malta	Paradise Papers - Malta corporate registry
TANTI QUALITY STREET LTD	31-DEC-1985	Malta	Malta	Paradise Papers - Malta corporate registry
BAYMONT STREET HOLDING B.V.	19-JAN-2016	Malta	Malta	Paradise Papers - Malta corporate registry
Rudolph Street	21-MAR-2010	Malta	Malta	Paradise Papers - Malta corporate registry
PAPER STREET	15-MAY-2012	Malta	Malta	Paradise Papers - Malta corporate registry

COMPANIES AT THE SAME REGISTERED ADDRESS IN MALTA (partial)

An advanced Reverse WHOIS search on the original company name “ExchangeXYZ” in the Country of Malta revealed more than 20 related domain names. Most of the websites have not been developed, while one is a cryptocurrency exchange to bet on professional sports events. It is entirely feasible that the site is a front for laundering proceeds.



REVERSE WHOIS LISTING OF COMPANIES RELATED TO EXCHANGEXYZ REGISTERED IN MALTA

Money Laundering for Tax Avoidance

According to the global companies database OpenCorporates, the oldest legally registered business for ExchangeXYZ was in Hong Kong, dated back to 2017. Database records show the Hong Kong entity currently inactive. However, ExchangeXYZ was very busy from the spring of 2018 to early 2019 establishing business entities in a dozen other countries.

Of greater note are the locations that are well-known offshore centers. In addition to Malta, they have established entities in Jersey, Uganda (well, maybe not so well-known), Singapore, and Switzerland.

Birch also notes that:

“Beneficial owners typically want to keep bank accounts nearby so they’re easier to use, or they may start accounts in places with banking secrecy like Switzerland or Liechtenstein. As a result, shell companies are often domiciled far from associated accounts.”

The Exchange also created three entities in India, the business name of one of which implies an investment in the clubs and resorts industry. The Exchange also has addresses in London.

THE LOCATION OF ONE OF EXCHANGEXYZ’S UK-BASED ENTITIES

The London addresses found in the companies incorporation record in OpenCorporates.com reveal residences. Indeed, the address pictured above has had eight other shell companies associated with it, according to the Panama and Paradise Papers.

Offshore Entities (8) Officers (5) Intermediaries (0) Addresses (415) Others (0)

	Incorporation	Jurisdiction	Linked To	Data From
A.O.3.T. OXPAHA TOMCK CORP.	30-MAY-1995	British Virgin Islands	United Kingdom	Panama Papers
HAYS MEWS PROPERTIES LIMITED	16-APR-1997	British Virgin Islands	United Kingdom	Panama Papers
HAYS MEWS ESTATES LIMITED	16-APR-1997	British Virgin Islands	United Kingdom	Panama Papers
Adams Mews Limited	28-JUN-2006	British Virgin Islands	United Kingdom	Panama Papers
3 Cumberland Ltd	28-APR-2006	British Virgin Islands	United Kingdom	Panama Papers
3 Cornell Square Limited	13-NOV-2009	British Virgin Islands	United Kingdom	Panama Papers
GAILMORE 3 LIMITED	18-JAN-2000	British Virgin Islands	United Kingdom	Panama Papers
Vaseq Bermuda 3, L.P.	15-SEP-2004	Bermuda	Bermuda, United Kingdom	Paradise Papers - Appleby

LIST OF SHELL COMPANIES ASSOCIATED WITH THE RESIDENCE ABOVE

Reverse WHOIS searches on each of the entity *names* of the offshore entities did not reveal any related domains; however, searches on Domain Names that included ExchangeXYZ and contained Registrant Contact:Country that included a country name (e.g., India) in some cases displayed domain names related to the ExchangeXYZ domain name. In the overwhelming number of instances in which domain names did display in the Reverse WHOIS results, the domains were inactive.

The circumstantial indicators discussed above should signal to consumers and regulators that business operations at ExchangeXYZ may not be in the best interest of its customers. Instead, it appears that ExchangeXYZ has created itself a financial ecosystem in which business occurs between entities.

Researchers could be forgiven if they were under the impression that the store of wealth the Exchange has accumulated may be stashed in far away and exotic locations. These locations lie beyond the reach of law enforcement authorities in the United States, the European Union, and even China. If and when the Exchange shutters its operations, consumers in the United States may lose hundreds of millions of dollars without legal recourse.

Beyond Cryptocurrency Exchange Fraud

Cryptocurrency fraud is not the only form of online financial crime investigators can apply WHOISXMLAPI.com's Domain Research Suite to. The FBI cited in its Internet Crime Report for 2019 that the year before had seen a dramatic spike in Internet-based theft and fraud. The report estimated that in 2018 in the United States alone, cybercriminals stole $2.7 billion from consumers and organizations.

WHOISXMLAPI.com's Domain Research Suite tools and traditional online investigative practices may not stop most of the crimes from happening. However, the integrated approach may help authorities and investors more readily get to the source of cryptocurrency and other forms of financial fraud on the Internet. Possibly, investment recovery rates may rise and the data collected during investigations may inform policymakers about viable ways to bring law and order to the Wild West of the Web.