BROKERCHOOSER

Unmasking Digital Deception:

A DATA-DRIVEN APPROACH TO MAPPING AND COMBATING ONLINE INVESTMENT FRAUD IN EUROPE

TABLE OF CONTENTS

ABOUT BROKERCHOOSER

Established in 2016, BrokerChooser is an independent, data-driven, and international platform specializing in brokerage comparisons. Utilizing a proprietary methodology, we rigorously **evaluate and test over 100 highly regulated brokers worldwide**, ensuring they are reliable and a robust choice for clients.

Our expert team is committed to protecting retail investors from scammers and fraudsters. To achieve this, we have developed innovative tools such as the 'Scam Broker Shield' and 'Scam Broker Alert' enabling users to verify the trustworthiness and regulatory status of online financial service providers, thus offering a crucial first line of defense against potential scams.

> *We have built a proprietary database that includes safety information and regulatory warnings on over 30,000 financial service providers worldwide and created articles on each of these entities.*

Using Google search data on our exclusive content, **we are in possession[1] of a globally unique dataset** that provides insights into the prevalence of online searches for investment scams and fraudulent service providers. Our research methodology ensures that these insights have an extensive geographical reach and closely approximate the actual searches conducted for these potentially fraudulent entities.

By unmasking actual fraudulent entities, we are hoping to provide much needed information to regulators and other stakeholders who apparently lack sufficiently detailed data to combat investment scams effectively.

Rooting out online investment fraud will necessitate involving more actors into the fight such as search engine operators, domain hosting companies as well as social media sites and finfluencers. Our goal is to empower them with information and data-driven insights.

---

[1] All the information made available by BrokerChooser is based on our proprietary database and professional methodology, which is unbiased, prepared in accordance with the best interest of our customers. and fully independent from the remuneration structure we have in place with our partners.

EXECUTIVE SUMMARY

This white paper examines the rising incidence of online investment scams and the proliferation of financial service providers of questionable reliability within the European context, driven by the digital transformation of the financial sector.

Analyzing data garnered from Google search results on **1.3 million articles in 56 languages** published by BrokerChooser, the report includes the following key findings:

1	**Scale of the problem**	The study identified 67 not-recommended entities targeting EU citizens, generating 1.3 million Google search impressions from European locations in the surveyed period.
2	**Geographical concentration**	Five EU member states (Germany, France, Poland, Italy, and the Netherlands) account for 86.4% of the total search volume, indicating either disproportionate targeting or heightened awareness in these regions.
3	**Fraudulent tactics**	The top 10 most searched entities, confirmed as displaying scam-like characteristics, demonstrate sophisticated operations targeting specific countries and claiming to use artificial intelligence (AI) and other advanced technologies to provide traders with decisive edge over the market.
4	**Assets advertised**	Cryptocurrency trading dominates the fraudulent offerings, with 6 out of 10 top scammers prominently featuring it. Other offerings include Forex, CFDs, real estate, and precious metals.
5	**Global reach**	The identified scams extend beyond the EU, attracting searches from over 50 non-EU countries.

By casting light on the operational tactics of these fraudulent entities, BrokerChooser aims to convert the abstract notion of "investment scams" into **precise, actionable intelligence**. Our objective is to equip authorities with data-driven insights that enable more focused and effective enforcement strategies. Our purpose is to bridge the gap between mere awareness and proactive measures, offering a clear framework for regulators to identify, scrutinize, and prosecute these malicious actors.

The **recommendations proposed in the paper focus on prevention** and are addressed to various stakeholders such as regulators, non-governmental organizations (NGOs) and corporate as well as industry actors that possess the authority and capabilities to combat this growing threat.

Our recommendations

1   Integration of regulatory warnings into search engine results

2   Enhanced scrutiny of digital advertising

3   Collaboration with domain hosting companies to disrupt fraudulent operations

4   Amplification of regulatory warning lists through public awareness campaigns

The research underscores the urgent need for coordinated action among regulators, technology companies, financial institutions, and other stakeholders to create a more robust defense against online investment scams in the EU. The findings and recommendations aim to foster a safer investment environment and protect EU citizens from financial fraud.

INTRODUCTION

The digital transformation of the financial sector has ushered in an era of unprecedented opportunities for investors, accompanied by a proportionate increase in the prevalence of online investment scams. This research report aims to elucidate the scope and nature of this growing threat, with a particular focus on how it is encountered by Europeans.

Recent data from authoritative sources underscores the magnitude of this issue. The Federal Bureau of Investigation's (FBI) Internet Crime Report 2023 indicates that investment fraud has become the most financially detrimental crime category in the United States, with losses escalating from $3.31 billion in 2022 to $4.57 billion in 2023, representing a 38% increase. Notably, cryptocurrency-related investment fraud exhibited a 53% surge, reaching $3.96 billion in 2023. Cumulatively, over the past five years, global losses attributed to scam victimization have amounted to $37.4 billion.

In comparison, Interpol's Financial Fraud Assessment report, which covers data from 196 member countries, presents an even more severe scenario. It estimates that in 2023, perpetrators of digital fraud embezzled over $1 trillion from victims worldwide. This scale is facilitated by technological advancements that enable transnational organized crime groups to target victims with unprecedented precision and scale.
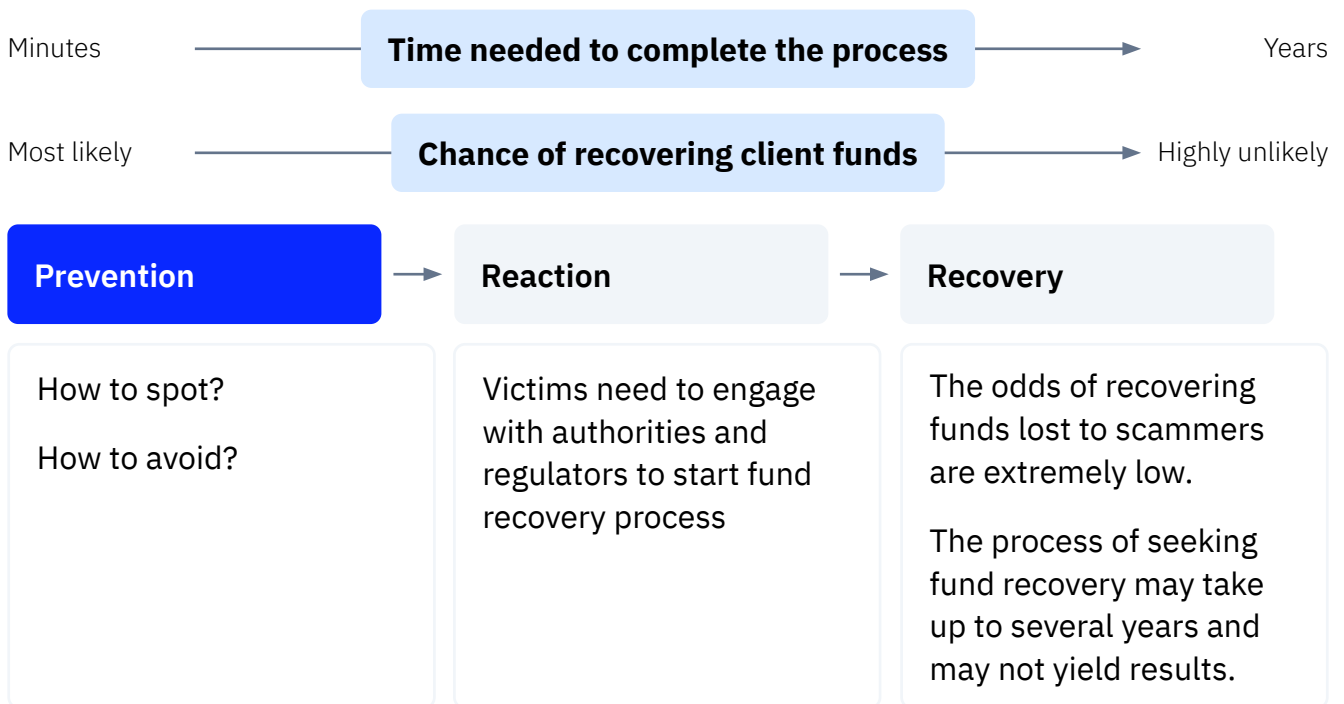
The European continent has not been immune to this global epidemic. Interpol reports a significant escalation in online investment frauds, phishing, and other financial fraud schemes within the region.

These operations are characterized by their transnational and often transcontinental nature, leveraging globalized information and communication technologies. Perpetrators increasingly employ emerging technologies, including Artificial Intelligence (AI) and deep fakes, to deceive victims and obfuscate their identities.

BrokerChooser embarked on writing this report with the objective of leveraging our globally unique data to produce highly informative and actionable insights.

We assert that the most effective phase in combating online investment scams is prevention. When the public is equipped with accurate information and the necessary tools to verify a service provider's safety, they can avoid falling victim to scams with minimal effort.

Why prevention is key in the fight against investment scams

Minutes	Time needed to complete the process	Years

Most likely	Chance of recovering client funds	Highly unlikely

Prevention →	**Reaction** →	**Recovery**
How to spot? How to avoid?	Victims need to engage with authorities and regulators to start fund recovery process	The odds of recovering funds lost to scammers are extremely low. The process of seeking fund recovery may take up to several years and may not yield results.

Informed users can protect their funds with just a few clicks. Conversely, once an individual has been defrauded, **the likelihood of recovering their funds plummets**, and any potential recovery process is exceedingly complex, protracted, and often spans several years.

The impetus for this research extends beyond mere data analysis. BrokerChooser is regularly contacted by users who have fallen victim to investment scams. These personal accounts of financial loss and emotional distress serve as a reminder of the human cost associated with fraudulent financial activities. The narratives of depleted life savings and profound psychological impact underscore the urgency of our mission and provide additional motivation for concerted action against these malicious entities.

Uniting forces in combating investment fraud

Our objective is twofold: to raise awareness about this pervasive issue and to propose actionable recommendations for mitigating the threat posed by these entities, thereby fostering a safer investment environment for all stakeholders.

We extend an invitation to regulators, non-governmental organizations, and industry bodies to collaborate in this endeavor to combat online investment scams. It is our conviction that only through coordinated, multi-stakeholder efforts can we effectively counteract financial fraud and safeguard the interests of investors across Europe.

GEOGRAPHICAL DISTRIBUTION OF INVESTMENT SCAMS AND NOT-RECOMMENDED SERVICE PROVIDERS IN EUROPE

This section presents an analysis of the geographical spread of the visibility of online investment scams and not-recommended financial service providers within the EU as reflected in Google searches. This unique set of data allows for a better understanding of geographical concentration and member states where user engagement is the highest.

Global and European context

On a global scale, the study identified **636 entities categorized as "not recommended" by BrokerChooser** in the case of which search volumes indicate a clear sign of user awareness.

Focusing specifically on Europe, the analysis revealed **67 such service providers targeting EU citizens across multiple member states.** These entities generated 1.3 million Google search impressions from EU countries during the surveyed period, indicating a visible level of interest or concern among EU residents.

Concentration of impact

An analysis of the data shows that the influence of these 67 entities extends across 26 out of 27 EU member states, albeit with varying degrees of intensity. A thorough legal examination[2] of the top 10 most frequently searched entities confirmed that all of them displayed scam-like characteristics. **Interestingly, 9 out of these 10 entities generate an exceptionally high search volume in a single EU country.** For instance, of the 129,251 search impressions triggered by Immediate Edge in the period analyzed, 60,233 come from French locations. This suggests targeted approaches that may exploit specific cultural or regulatory environments.

The data reveals a significant concentration of searches, with the top 10 scam-like entities (approximately 15% of the identified entities) accounting for more than half of all related searches. This concentration suggests that a small number of sophisticated operations are responsible for a disproportionate amount of potentially fraudulent activity.

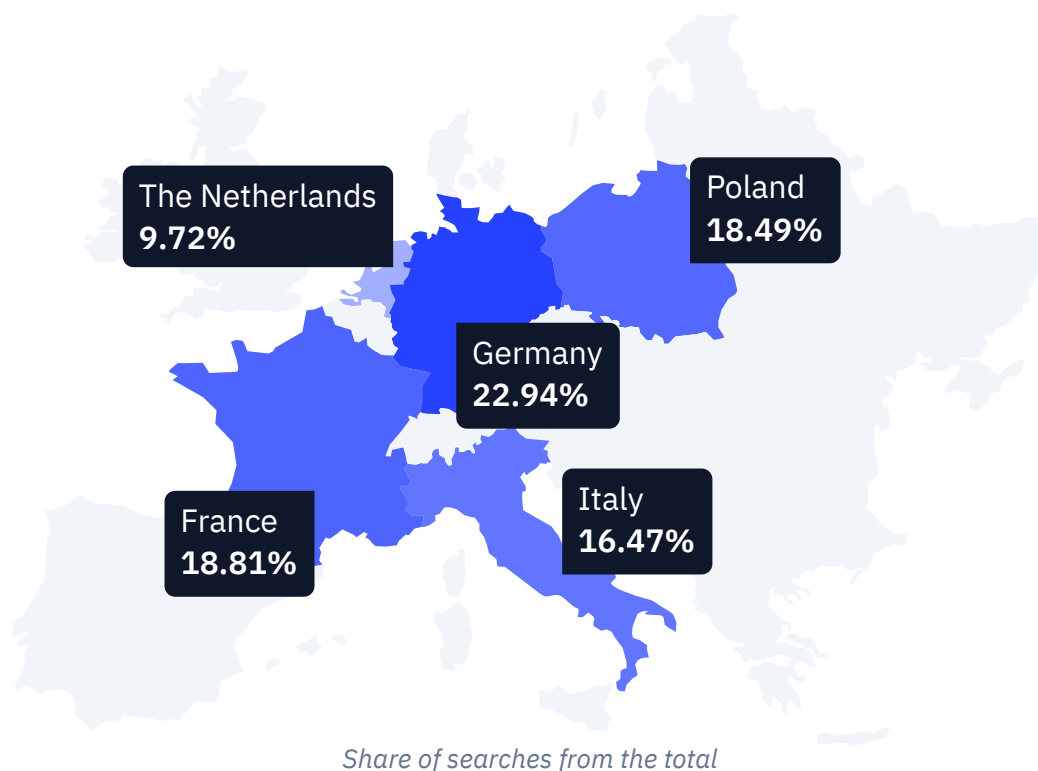[2] See the chapter entitled 'Top 10 most searched scammer entities'

It is also noteworthy that these 10 entities are not exclusively targeting EU countries. The global dataset indicates that individuals from more than 50 non-EU countries also conducted searches for these entities during the surveyed period.

Most affected countries

The analysis of this data reveals striking patterns in the distribution of online investment scam-related searches across the EU.

The search patterns demonstrate a **remarkable concentration within a small subset of EU member states**. This localization of search activity suggests that certain countries may be disproportionately targeted by scammers or have populations more actively seeking information about potential fraudulent schemes.

Notably, five EU member states account for 86.4% of the total search volume, amounting to 1.3 million search impressions. The distribution among these countries is as follows:

The Netherlands
9.72%

Poland
18.49%

Germany
22.94%

France
18.81%

Italy
16.47%

Share of searches from the total

These countries represent **some of the largest economies in the EU**, potentially making them more attractive targets for scammers due to greater wealth concentration. Additionally, the better availability of scam-related information in major European languages (German, Italian, French, Spanish) might facilitate higher search volumes in these countries.

This ranking of most affected countries provides valuable insights for policymakers and regulatory bodies, highlighting areas where efforts to combat online investment scams might be most urgently needed or where interventions could have the most significant impact.

TOP 10 MOST SEARCHED SCAM-LIKE ENTITIES

The in-depth examination of the data yielded a ranking of the most searched for entities in the EU that BrokerChooser advises against. These entities were subjected to rigorous scrutiny to provide a comprehensive understanding of their operations and potential risks to investors.

To ensure the utmost accuracy and reliability in our assessments, each of these entities underwent a meticulous legal and operational evaluation. Our comprehensive due diligence process encompassed a wide array of critical factors, including:

1

Website (design, structure and available information) analysis and digital presence evaluation

2

Scrutiny of contact information and other publicly available data about each entity

3

Jurisdiction and regulatory information evaluation and verification

4

Review and evaluation of any existing regulatory warnings or alerts as well as negative news associated with these entities

5

Investigation into the level of corporate transparency (including entity's purported foundation date, corporate structure, ownership information and senior management information)

6

Legal transparency assessment (including the review of key customer contracts, service agreements Anti-Money Laundering (AML) and Know Your Customer (KYC) policies and practices)

7

Authenticity and integrity of product offering (e.g. bonus offerings, heavy incentivization of trading, understatements of the risk associated with trading, excessive leverage etc)

This multifaceted approach allowed for a holistic evaluation of each entity, to differentiate legitimate operations from fraudulent schemes. By cross-referencing and corroborating information across multiple sources and regulatory databases, we have established a robust framework for identifying red flags and inconsistencies that are hallmarks of fraudulent operations.

Based on this rigorous methodology, we can assert with a high degree of confidence that all 10 entities identified in our study exhibit characteristics of fraudulent operations.

These entities display a lack of transparency, absence of proper licensing, misrepresentation of services, and a conspicuous deficiency in legitimate business practices.

The cumulative evidence strongly suggests that these operations have no genuine intention of providing bona fide financial services to their purported customers.

The following entities have been identified as the most frequently searched, suggesting they may pose the greatest risk to potential investors:

Name of entity	Featured on the warning list of the following regulatory bodies
1 **Immediate Edge**	FCA
2 **Pocket Option**	IOSCO
3 **Quantum Ai Trading**	IOSCO
4 **T4Trade**	IOSCO
5 **Bit Lidex 360 /Bitsoft 360**	CSSF / IOSCO
6 **Roboforex**	IOSCO
7 **Apex Bitcoin Mining**	FCA

Name of entity	Featured on the warning list of the following regulator(s)
8 Mountain Wolf	FCM
9 Igenius Fx	FCA / IOSCO
10 Real Fx	CTFC / FCA

<div align="right">

More info in appendix

</div>

By naming and detailing the modus operandi of these fraudulent operations, **we strive to transform the abstract concept of "investment scams" into concrete, actionable intelligence.** Our goal is to empower authorities with specific, data-driven insights that can inform more targeted and effective enforcement strategies. This approach seeks to bridge the gap between awareness and action, providing a clear roadmap for regulators to identify, investigate, and prosecute these harmful entities.

ASSETS ADVERTISED BY THE TOP SCAM-LIKE ENTITIES

The analysis of the top 10 most prevalent entities identified as displaying scam-like characteristics operating within the EU reveals a clear pattern in their purported asset offerings. This examination provides insights into the strategies employed by these potentially fraudulent operations to lure unsuspecting investors.

Cryptocurrency: the dominant lure

Our research shows an overwhelming prevalence of cryptocurrency-related assets among these fraudulent entities. **Six out of the top 10 feature cryptocurrency trading as their primary service.**

This dominance of crypto-based schemes is not surprising, given the complex and often misunderstood nature of digital assets. Scammers exploit the allure of cryptocurrencies, **capitalizing on their reputation for rapid value appreciation** and the general public's limited understanding of the underlying technology.

> *These entities increasingly employ deceptive claims regarding the use of artificial intelligence (AI) and other advanced technologies, purporting to provide traders with a significant competitive advantage through the application of sophisticated algorithms and machine learning techniques.*

They allege that the capabilities of their systems include predictive market analysis with unprecedented accuracy, real-time processing of vast quantities of financial data and autonomous decision-making for optimal trade execution.

By promising unrealistic returns and leveraging the 'fear of missing out' on the next big boom, **these entities effectively target both novice investors and those seeking high-risk, high-reward opportunities.**

While cryptocurrency trading emerges as the clear front-runner, the remaining four entities in our top 10 list showcase a diverse array of assets their clients can purportedly trade. This eclectic mix includes:

Forex (FX) Trading

appealing to those interested in currency market speculation.

Contracts for Difference (CFDs)

targeting investors looking for leveraged trading opportunities across various markets.

Real estate

attracting those seeking tangible, long-term investment options.

Precious metals (e.g. gold)

capitalizing on the traditional safe-haven appeal of physical commodities.

We collected the product information displayed on the websites of the top 10 entities featured in our report.

Name of entity	Product information	Additional information
Immediate Edge	AI trading software Immediate Edge is an advanced automated trading platform designed for cryptocurrency trading. Crypto trading platform. Disguised as a free educational site but its aim is to lure you into crypto trading.	N/A
Pocket Option	CFDs Binary options	N/A
Quantum Ai Trading	Quantum AI is a cutting-edge software that combines quantum computing with artificial intelligence (focus is on crypto trading). Crypto trading platform / trading bot offering disguised as an educational site.	N/A

Name of entity	Product information	Additional information
T4Trade	CFDs	N/A
Bit Lidex 360 / Bitsoft 360	Crypto	N/A
Roboforex	FX	Offering rebates, cashbacks, bonuses and leverage up to 1:2000
Apex Bitcoin Mining	FX and cryptocurrency broker Professional trading & investment company with emphasis on cryptocurrency, forex, binary option, CFDs.	Offering fix weekly returns of 15-50%
Mountain Wolf	Crypto exchange	N/A
Igenius Fx	FX, real estate, gold, crypto trading, retirement + financial planning Crypto, FX, precious metals, indices, stocks, commodities, shares etc.	Notice you receive when you open the website in browser: "Notice:All trades placed and investments are 100% secured so traders should be 100% confident as there will be always success in trade."
Real Fx	N/A	Offering instant cashbacks, trading bonuses if you deposit

By pretending to be offering a broad spectrum of investment options, these entities cast a wider net, aiming to capture the interest of diverse investor profiles. The inclusion of traditional assets like real estate and gold alongside more modern financial instruments like CFDs suggests an attempt to present a façade of legitimacy and diversification.

The diversification of asset offerings allows scammers to pivot quickly in response to changing market sentiments or regulatory scrutiny while providing an air of sophistication and comprehensive financial services.

RECOMMENDATIONS

Based on our comprehensive analysis of online investment scams in the EU, we propose the following recommendations to strengthen fraud prevention measures and enhance investor protection. The proposed interventions are targeted at various stakeholders possessing the necessary capabilities and resources to counteract the proliferation of online investment fraud.

Integration of regulatory warnings in search engine results - search engine operators

We advocate for the development and implementation of a system that **incorporates regulatory warning lists into major search engines.** This integration would enable the automatic display of prominent warning signs alongside search results featuring entities included in these lists. Such a mechanism would significantly enhance the visibility of regulatory warnings at a critical decision-making point for potential investors, thereby reducing the likelihood of engagement with fraudulent entities. During the COVID-19 pandemic, Google applied similar warnings to highlight misinformation, which proved effective in guiding users away from unreliable sources.

Enhanced scrutiny of digital advertising - digital platforms

A more rigorous approach to monitoring and analyzing paid advertisements from potentially fraudulent entities. We recommend leveraging advanced data analytics techniques **to examine the financial transaction data associated with these advertisements.** This analysis could provide valuable insights into the individuals or businesses orchestrating these scams, facilitating more effective identification and prosecution of perpetrators.

Collaborative efforts with domain hosting companies - hosting companies

We propose establishing a formalized collaboration framework between regulatory bodies and domain hosting companies. This partnership would aim **to expedite the process of discontinuing hosting services for URLs associated with identified fraudulent entities or scammers.** By disrupting the online presence of these operations, authorities can significantly impede their ability to attract and defraud potential victims.

Amplification of regulatory warning lists through public awareness campaigns - regulators and the media

Our research indicates that current regulatory warning lists have limited impact on investor behavior. For instance, Immediate Edge, identified as a top scamming entity in our analysis, has been featured on the UK's Financial Conduct Authority's warning list since 2020[3], yet continues to operate. Similarly, the Spanish regulator has issued a warning on Pocket Options (also included in our top 10 list) in 2019[4]. To address this issue, we recommend **the development and implementation of targeted public awareness campaigns** designed to increase the visibility and efficacy of these regulatory warning lists.

These campaigns should employ a multi-faceted approach, utilizing various media channels and leveraging partnerships with financial institutions, educational establishments, and consumer protection organizations. The objective is to elevate public consciousness regarding the existence and importance of these warning lists, thereby enhancing their preventative impact.

[3] https://www.fca.org.uk/news/warnings/immediate-edge
[4] https://www.cnmv.es/Portal/ResultadoBusqueda.aspx?tipo=1&nombre=pocketoption.com

CONCLUSION

This white paper sheds light on the widespread problem of online investment scams, with a focus on Europe. We've leveraged BrokerChooser's unique dataset and proprietary research methods to offer in-depth insights into these fraudulent activities' scope and impact.

Our findings reveal that the fight against online investment scams involves numerous stakeholders, including regulators, search engine operators, domain hosting companies, and social media platforms. It is clear that combating this growing threat requires a multi-faceted approach. We hope our report highlights the critical areas where effective measures can be implemented to prevent individuals from falling victim to these schemes.

Ultimately, our goal is **to empower all stakeholders with actionable, data-driven insights** that not only raise awareness but also facilitate proactive measures against investment fraud. By working together, we can create a safer investment environment and protect the interests of investors across Europe.

Contact the authors

We welcome suggestions and feedback related to the findings of this report. If you have any questions or would like to receive more information, feel free to reach out to the authors.

Dan Sallai
Chief Marketing Officer
dan.sallai@brokerchooser.com
LinkedIn

Edith Balázs
Senior Content Editor
edith.balazs@brokerchooser.com
LinkedIn

Zoltán Kormányos
General Counsel
zoltan.kormanyos@brokerchooser.com
LinkedIn

APPENDIX

Methodology

Methodology for assessing recommended brokers

BrokerChooser employs a meticulous methodology to evaluate and rank more than 100 online brokers globally. This comprehensive process involves assessing brokers based on over 600 individual data points across nine key areas: fees, safety, ease of account opening, education, trading platforms, product portfolio, customer service, research tools, and mobile trading experience.

Each broker is tested through live accounts using real money to ensure accuracy and reliability. The methodology is refined annually, integrating feedback from both the team's analyses and user experiences. This rigorous approach ensures an objective and transparent comparison, helping investors make informed decisions[5].

We only recommend brokers that operate under top-tier regulation to ensure our customers experience the highest level of safety, security, and reliability in their investment activities. This guarantees that the brokers adhere to stringent regulatory standards, providing a trustworthy and transparent trading environment.

Data collection for the present report

This report utilizes Google Search impression data based on 1.3 million articles published in 56 languages on the BrokerChooser website. The overall purpose of these articles is to indicate to readers whether a specific entity is trustworthy or a fraudulent[6] business. The articles are powered by a proprietary database that incorporates safety data and information featured in publicly available regulatory warning lists, from 12 financial market regulators and international organizations[7].

---

[5] Further information: https://brokerchooser.com/methodology
[6] Example: https://brokerchooser.com/safety/immediate-edge-broker-safe-or-scam
[7] The warning lists of the following regulators are included in the database: Commodity Futures Trading Commission (CFTC), Financial Conduct Authority (FCA), the Cyprus Securities and Exchange Commission (CySEC), the Autorité des Marchés Financiers (AMF), the Swiss Financial Market Supervisory Authority (FINMA), the Australian Securities and Investments Commission (ASIC), the Financial Industry Regulatory Authority (FINRA), the U.S. Securities and Exchange Commission (SEC), the Federal Financial Supervisory Authority (BaFin), the Comisión Nacional del Mercado de Valores (CNMV), the Alberta Securities Commission (ASC), and the International Organization of Securities Commissions (IOSCO).

The report uses data from articles that appear on the first page of Google search results. This serves as a proxy of the search volume for the entities featured in these articles. This high visibility correlates strongly with public awareness and recognition of these entities among the general population.

The data analyzed in this report covers the first 6 months of 2024. We restricted our analysis to service providers that averaged at least 5 searches per day in a specific country over the first six half of 2024.

Rationale for using these metrics

Extensive reach

The articles considered in this study appear on the first page of Google search results for an unprecedentedly wide range of names in most of the countries globally.

Correlation with Search Volume

First-page impressions closely approximate actual search volume, as appearance on the first page of Google search results is almost equal to the amount of searches that goes to that keyword.

Exclusive Data Access

BrokerChooser is in the possession of this unique data setting us apart from other entities that lack either the comprehensive database or the requisite level of trust.

This exclusive capability enables us to provide uniquely valuable insights and formulate informed recommendations for stakeholders.

Categorization of the top 10 entities in the EU

Each service provider included in this analysis was subjected to thorough legal scrutiny. This process involved verifying the entity's website and associated URLs, contact information, operational jurisdiction, regulatory compliance, licensing claims, and authenticity.

Additionally, we examined whether the entity appeared on any regulatory warning lists. We also investigated the entity's foundation date, historical operations, corporate structure, ownership transparency, and senior management credentials. Key customer contracts, service agreements, and Anti-Money Laundering (AML) and Know Your Customer (KYC) policies and practices were also assessed.

DETAILED INFORMATION ON THE TOP 10 SCAM-LIKE ENTITIES

1 Immediate Edge

Websites

http://www.immediateedgebot.com/
(browser says it is not safe)

https://immediate-edge.co/

https://immediateedgeapp.org/

https://immediateedge.ai/
(not working)

https://immediateedgepro.com/
(not working)

https://immediateedgeai.com/

https://official-immediateedge.com/

https://immediateedge-uk.com/
(website is blocked)

Contacts

info@immediateedgebot.com

support@immediateedgeapp.org

info@official-immediateedge.com

info@immediate-edge.co

Jurisdiction information
N/A

Licence information
N/A

Regulatory warning

https://www.fca.org.uk/news/warnings/
immediate-edge

https://register.fca.org.uk/s/unautho-
rised-firm?id=0014G00002TpGPsQAN

Foundation date
N/A

Corporate information
N/A

Ownership information
N/A

Senior management information
N/A

Key customer contracts

https://immediateedgeapp.org/
terms-of-use/

https://immediateedgeai.com/
general-terms/

https://immediate-edge.co/terms/

AML/KYC policy
N/A

2   **Pocket Option**

Websites
https://pocketoption.com/en

Foundation date
2017

Contacts
https://pocketoption.com/en/contacts/

Corporate information
Infinite Trade LLC

Jurisdiction information
Infinite Trade LLC a company registered in Costa Rica *(address seems to be fake)*

Ownership information
N/A

Senior management information
N/A

Licence information
Seemingly fake and illegible document uploaded onto the website claiming that it has a brokerage licence with the Mwali International Sevices Auhtority. The authority's register featured on an apparently shady website does not contained such busiess entity.

Key customer contracts
https://pocketoption.com/en/public-offer/

AML/KYC policy
https://pocketoption.com/en/aml-policy/

Regulatory warning
https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal&RegulatorID=0&JurisdictionID=0&SubjectID=0&Keywords=pocket

3 Quantum Ai Trading

Websites

https://quantumaiplatform.com/

https://quantum-ai.trading/
(not working)

https://quantum-ai.in/
(website is blocked)

https://quantumai.bot/

https://thequantumai.app/
(browser says it is not safe)

https://quantumaiapp.ai/
(not working)

https://quantum-ai.com.au/
(not working)

Contacts
44(20)35970879
info@quantumai.bot

Jurisdiction information
UK phone number, registered address is a fake Singapore address

Licence information
N/A

Regulatory warning
https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal&-RegulatorID=0&JurisdictionID=0&SubjectID=0&Keywords=Quantum+AI

Foundation date
N/A

Corporate information
N/A

Ownership information
N/A

Senior management information
https://quantumaiplatform.com/team/
(obviously fake)

https://quantumai.bot/team/
(obviously fake)

Key customer contracts
https://quantumaiplatform.com/terms-of-use/

AML/KYC policy
N/A

4   T4Trade

Websites
https://www.t4trade.com/en/

Contacts
compliance@tradeco.sc

Jurisdiction and licence information
Tradeco Limited is an entity holding securities dealer licence issued by the Seychelles Financial Services Auhtority

Regulatory warning
https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal&RegulatorID=0&JurisdictionID=0&SubjectID=0&Keywords=T4Trade

Foundation date
N/A

Corporate information
Tradeco Limited

Ownership information
N/A

Senior management information
N/A

Key customer contracts
https://www.t4trade.com/wp-content/uploads/2024/04/1.-T4T_Client_Services_Agreement_v.2024-001.pdf

AML/KYC policy
N/A

5   Bit Lidex 360 /Bitsoft 360

Websites

https://bitlidex360.com/

https://bitlidex360.org/
(not working)

https://bitsoft360.io/

https://bitsoft360.net/

https://bitsoft360.com/
(not working)

Contacts
N/A

Jurisdiction and licence information
Fake Scottisch company (Trading Funnels Ltd) with fake address

Fake UK company called Bitsoft360 LTD with fake address

License information
N/A

Regulatory warning
https://www.cssf.lu/en/2023/07/warning-concerning-the-fraudulent-activities-carried-out-by-the-entity-bit-lidex-360/

https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal&id=28862&entity=Fraudulent-online-trading-platforms

Foundation date
N/A

Corporate information
N/A

Ownership information
N/A

Senior management information
N/A

Key customer contracts
N/A

AML/KYC policy
N/A

6 Roboforex

Websites
https://roboforex.com/

Contacts
https://roboforex.com/about/company/
contacts/

Jurisdiction information
Belize

License information
Claims to be licensed by the Belize Financial
Services Commission under licence number
of 000138/7 but this cannot be verified on
the regulator's website.

Regulatory warning
https://www.iosco.org/v2/investor_
protection/?subsection=investor_alerts_

Foundation date
N/A

Corporate information
N/A

Ownership information
N/A

Senior management information
N/A

Key customer contracts
N/A

AML/KYC policy
N/A

7   Apex Bitcoin Mining

Websites
https://apexbitcoinmining.com/
(not working)

https://apexbitmining.com/
(not working)

https://apexbitmintrade.com/
(browser says it is not safe)

https://apex-financetrade.com/

https://www.apexmining.pro/

Contacts
info@apexbitcoinmining.com

support@apex-financetrade.com

support@apexmining.pro

+1 (659) 7589074
(Alabama phone number)

Jurisdiction and licence information
In the FAQ section it is referred to as a
UK company, the phone number is from
Alabama US, anf their registered address
within the Terms is a fake Detroit address

License information
N/A

Regulatory warning
https://www.fca.org.uk/news/warnings/
apex-bitcoin-mining

Foundation date
N/A

Corporate information
Only fake

Ownership information
N/A

Senior management information
N/A

Key customer contracts
https://apex-financetrade.com/terms-and-
conditions.html

https://www.apexmining.pro/about.html

AML/KYC policy
N/A

8 Mountain Wolf

Websites
https://www.mountainwolf.com/

Contacts
support@mountainwolf.com

Jurisdiction information

Mountain Wolf s.r.o. (Slovakia - claiming to have VASP licence but it is not present in the register of the National Bank of Slovakia)

MOUNTAIN WOLF PSP FZCO (UAE - claiming to have payment service provider license - no such license can be found at VARA, Central Bank of UAE and at the SCA + financing broker exchange expired according to the register of the Government of Dubai)

MOUNTAIN WOLF LLC (a Georgia entity claiming to have license to provide virtual assets services, custodian services, payment services, and foreign exchange services but it is not registered with the National Bank of Georgia)

TOO Mountain Wolf (a Kazakh entity caliming to be entitled to provide financial services inlcuding FX, crypto and electronic wallet but it cannot be found in the register)

License information
https://www.mountainwolf.com/legalNotice.html

Regulatory warning
https://www.fma.gv.at/en/mountain-wolf/

Foundation date
2019

Corporate information
https://www.mountainwolf.com/legalNotice.html

Ownership information
N/A

Senior management information
N/A

Key customer contracts
N/A

AML/KYC policy
https://www.mountainwolf.com/media/GTS%2020230928.pdf

9 Igenius Fx

Websites
https://www.igenius-fx.com/

https://igeniusuniversal.com/index.html

https://fxgenius.com/

http://www.igeniusfx.com/
(not working)

Contacts
support@fxgenius.com

Jurisdiction information
Fake company + fake certificate of incorporation is uploaded onto the website under the name of Igenius Global Limited

License information
N/A

Regulatory warning
https://www.fca.org.uk/news/warnings/igenius-fx

https://www.iosco.org/v2/investor_protection/?subsection=investor_alerts_portal&id=25521&entity=Igenius-FX

Foundation date
2016

Corporate information
N/A

Ownership information
N/A

Senior management information
https://www.igenius-fx.com/teams
(totally fake team page)

Key customer contracts
https://www.igenius-fx.com/legal

https://fxgenius.com/legal-documents/

AML/KYC policy
https://fxgenius.com/legal-documents/

10 Real Fx

Websites
http://www.realforexr.com/
(not working)

https://www.realfxmarket.com/Index

Contacts
support@realfxmarket.com

Jurisdiction information
Stealing the name and referring to a legit company as license holder (Real Finance Ltd) which is a property development financing company.

Also referring to a fake non-existent UK company (RealfxMarket UK Limited) as the owner of the website.

License information
N/A

Regulatory warning
https://www.cftc.gov/node/221106

https://register.fca.org.uk/s/unauthorised-firm?id=0014G00003BrChFQAV

Foundation date
N/A

Corporate information
N/A

Ownership information
N/A

Senior management information
N/A

Key customer contracts
N/A

AML/KYC policy
N/A

BrokerChooser

2024