Binary Options Fraud: Understanding the Risks, Identifying Scams, and Protecting Your Investments

Executive Summary

Binary options, financial instruments based on a simple yes/no proposition regarding an underlying asset's price movement, have become a significant area of concern due to widespread fraudulent activity. While legitimate, regulated binary options exist and trade on specific US exchanges under regulatory oversight, the vast majority of the market operates through unregulated, often offshore, internet-based platforms. These platforms are frequently used to perpetrate scams characterized by manipulative practices, refusal to return client funds, and identity theft. Common tactics include manipulating trading software to ensure client losses, aggressively promoting unrealistic returns, employing high-pressure sales tactics by fake "brokers," using deceptive bonus offers to lock funds, and obstructing or refusing withdrawals. Financial regulatory authorities globally, including the SEC and CFTC in the US, the FCA in the UK (which banned retail sales), ESMA in the EU (leading to national bans), and ASIC in Australia (which also banned retail sales), have issued numerous warnings and taken enforcement actions against fraudulent operators. Case studies involving firms like Spot Option, Yukom Communications (BinaryBook), and Jonathan Cartu (Blue Moon Investments) illustrate the scale and methods of these scams, often involving tens or hundreds of millions of dollars in investor losses. Engaging with fraudulent binary options schemes carries substantial risks, including the near certainty of total loss of invested capital, exacerbated by payout structures inherently favoring the platform and outright fraud. Protecting oneself requires rigorous due diligence, primarily verifying the registration and regulatory status of any platform through official channels provided by regulators like the CFTC, SEC, FCA, and ASIC, and avoiding unregistered or offshore entities entirely. Victims should immediately cease contact with scammers, notify their financial institutions, and report the fraud to relevant regulatory and law enforcement bodies, utilizing resources like the CFTC/SEC complaint portals, the FBI's IC3, the UK's FCA and Action Fraud, EU national regulators, and Australia's ASIC and Scamwatch. Vigilance, skepticism towards high-return promises, and reliance on regulated entities are paramount to avoiding victimization.

related posts : Best Binary Options Brokers (in 2025)

1. Understanding Binary Options: Legitimate vs. Illegitimate

Binary options have garnered significant attention, both as a speculative financial tool and, more prominently, as a vehicle for widespread financial fraud. Understanding the fundamental nature of these instruments, how they operate in a legitimate context, and the critical differences from their fraudulent counterparts is essential for investor protection.

1.1. Defining Binary Options: The "Yes/No" Proposition

At its core, a binary option is a type of financial derivative based on a simple "yes or no" proposition concerning a future event, typically related to the price movement of an underlying asset.[1] The question might be whether the price of a specific stock, commodity, currency pair, or market index will be above or below a predetermined level (the strike price) at a specific future time (the expiration time).[5]

The term "binary" reflects the two possible outcomes for the option holder at expiration.[2] If the trader's prediction about the asset's price movement relative to the strike price is correct at the moment of expiration, the option expires "in the money," and the trader receives a predetermined, fixed payout.[1] Conversely, if the prediction is incorrect, the option expires "out of the money," and the trader typically loses the entire amount they paid to purchase the option (the premium).[2] This "all-or-nothing" payout structure is a defining characteristic.[3]

Binary options can be based on a wide range of underlying assets, including individual stocks, stock indices (like the S&P 500), commodities (like gold or oil), and foreign currency (forex) pairs (like EUR/USD).[5] Some platforms have even offered options based on specific events.[15]

A critical parameter is the expiration time and date.[2] This is the precise moment when the condition (price above/below strike) is evaluated to determine the outcome. Expiration periods can vary significantly, ranging from weekly or daily down to hourly or even just a few minutes.[8] The extremely short durations offered by many platforms contribute significantly to their speculative, gambling-like nature.[3]

The apparent simplicity of the yes/no question and the clearly defined potential profit or loss make binary options seem appealing, particularly to individuals new to financial markets or seeking quick results.[5] This superficial attractiveness, however, masks considerable risk. Predicting short-term market movements with the accuracy required for consistent profitability is exceptionally difficult, even for experienced professionals.[11] Furthermore, the inherent structure often carries a statistical disadvantage for the trader, akin to a "house edge" in gambling.[3] It is precisely this combination of apparent simplicity and underlying risk that fraudulent operators exploit, marketing binary options as easy investment opportunities while concealing the high probability of loss and the often-manipulated nature of their platforms.[12]

1.2. How Legitimate Binary Options Work (Exchange-Traded, Regulated)

While the binary options landscape is heavily populated by fraudulent actors, it is important to recognize that legitimate binary options trading has existed within regulated frameworks, primarily in the United States. These operations differ significantly from the common online scams.

In the US, binary options have been permitted to trade on specific exchanges registered with and overseen by regulatory bodies like the Commodity Futures Trading Commission (CFTC) or the Securities and Exchange Commission (SEC).[4] Key examples include the North American Derivatives Exchange (Nadex) and, historically, the Chicago Board Options Exchange (CBOE).[6] The Chicago Mercantile Exchange (CME) also introduced "event futures," which function similarly to binary options.[6] Trading on these regulated venues means operating under established rules and oversight, designed to ensure market integrity and investor protection.[9]

The pricing of binary options on these regulated exchanges is dynamic, typically ranging between $0 and $100 per contract.[6] The price reflects the market's collective assessment of the probability that the option's condition will be met at expiration. As traders buy ("bid") and sell ("ask"), the price fluctuates based on supply and demand, much like other financial markets.[1] The price paid by the buyer represents their maximum risk, while the difference between the price and $100 represents the maximum potential profit (before fees).[10] Conversely, for the seller, the price received represents their maximum potential profit, while the difference between the price and $100 is their maximum risk.[15]

A crucial feature of regulated exchange trading is the mitigation of counterparty risk. The exchange often acts as a central counterparty or utilizes a central clearinghouse, ensuring that obligations are met even if one party defaults. Furthermore, all trades are fully collateralized, meaning both the buyer and seller must commit capital upfront to cover their potential maximum loss on the contract.[15] This structure prevents the direct conflict of interest seen in many unregulated platforms where the platform itself is the counterparty to the client's trade.

Transparency is another hallmark of regulated trading. Contracts are typically standardized with clear specifications regarding the underlying asset, strike price, and expiration.[15] Trading rules and price movements are visible, operating within a framework of regulatory compliance.[10]

While often used for speculation, exchange-traded binary options can, in theory, be used for hedging purposes, allowing traders to protect existing positions against adverse price movements, although this is less common than with traditional vanilla options.[6]

The existence of this regulated market provides essential context. It demonstrates that the binary option *concept* is not inherently fraudulent. However, the *vast majority* of binary options trading, particularly that accessible globally online, occurs outside these regulated environments.[2] The key distinctions lie in regulatory oversight, transparent market-driven pricing, risk mitigation through clearing and collateralization, and the absence of a direct conflict of interest between the platform and the trader. The very limited number of authorized venues in the US [4] stands in stark contrast to the thousands of unregulated online platforms [4], highlighting where the primary risks of fraud reside. In the unregulated model, the platform typically acts as the direct counterparty [20], meaning it profits directly when its clients lose [21], creating a powerful incentive for the fraudulent practices detailed later in this report.

1.3. Table: Key Differences: Regulated vs. Unregulated Binary Options

To clarify the distinctions, the following table compares key features of regulated, exchange-traded binary options versus those typically found on unregulated online platforms:

Feature	Regulated Exchange-Traded	Unregulated Online Platform
Regulation	Overseen by bodies like CFTC/SEC (US)	Often unregistered, based offshore, lacks effective oversight
Platform	Designated Contract Market (DCM) or Registered Exchange	Private website/platform, often proprietary
Pricing	Market-driven (bid/ask), \$0-\$100 range, reflects probability	Often set by the platform, potentially manipulated
Payout	Fixed (\$100 or \$0 settlement)	Fixed percentage return (often <100%), or total loss; payout structure may be

		manipulated
Counterparty	Other traders (via exchange/clearinghouse)	Typically the platform itself (direct conflict of interest)
Transparency	Standardized contracts, public rules, regulatory oversight	Often opaque, terms can be complex/misleading, lack of oversight
Risk Disclosure	Mandated risk warnings	Often downplayed or misrepresented (e.g., "guaranteed returns")
Recourse	Regulatory channels, dispute resolution mechanisms	Extremely limited, especially if offshore

This comparison underscores the fundamental differences in structure, oversight, and inherent conflicts that make the unregulated binary options space particularly susceptible to fraud.

2. The Anatomy of a Binary Options Scam

The prevalence of fraud within the binary options market is staggering, largely facilitated by the structure of the online, often unregulated, environment in which most of these operations exist. Understanding how these scams are structured and the specific tactics employed is crucial for recognizing and avoiding them.

2.1. The Prevalence of Fraud: Unregulated Platforms and Offshore Operations

A defining characteristic of the binary options market is that a significant portion operates through internet-based trading platforms that do not comply with applicable regulatory requirements, particularly in major financial markets like the US, UK, EU, and Australia.[2] Many of these platforms are deliberately established in offshore jurisdictions with lax regulatory oversight or where enforcement is difficult.[14] This proliferation of unregulated online platforms has directly led to a surge in fraud complaints received by regulators worldwide.[13]

Operating offshore provides scammers with significant advantages. It makes it challenging for regulators in the victims' home countries (like the SEC, CFTC, or FCA) to assert jurisdiction, conduct investigations, freeze assets, or enforce judgments.[2] Investors dealing with these entities find they have minimal legal recourse or protection if things go wrong.[14]

The scale of this fraudulent activity is immense. The U.S. Federal Bureau of Investigation (FBI) has estimated that binary options scammers steal approximately US$10 billion annually on a global scale.[3] Data from the FBI's Internet Crime Complaint Center (IC3) showed a dramatic increase in reported complaints and losses between 2011 and 2016, rising from just four complaints with $20,000 in losses to hundreds of complaints involving millions of dollars annually, acknowledging that these figures likely represent only a fraction of the actual fraud.[4] Some European nations reported that binary options fraud accounted for up to 25% of all fraud complaints received during peak periods.[27]

Furthermore, investigations, particularly originating from extensive reporting in Israel (a historical hub for the industry), have linked many binary options operations to organized criminal syndicates.[3] This indicates a level of sophistication and organization far beyond isolated incidents of misconduct. The move to online, offshore platforms is not accidental; it is a calculated strategy to maximize reach while minimizing accountability, allowing a global criminal enterprise to flourish at the expense of unsuspecting investors.

2.2. Common Scam Mechanisms and Tactics

Fraudulent binary options operators employ a range of deceptive and manipulative tactics designed to lure investors and ensure the misappropriation of their funds. Key mechanisms include:

- **Manipulated Trading Platforms and Software:** This is a cornerstone of many binary options scams. Instead of facilitating fair trading, the platforms themselves are engineered to guarantee client losses.[4] Operators may distort the price feeds of underlying assets, ensuring that trades settle unfavorably for the client.[4] They might manipulate the payout calculations or the displayed results.[20] A particularly egregious tactic involves arbitrarily extending the expiration time of a trade that is currently "winning" for the client until the price moves against them, turning it into a loss.[4] Case evidence confirms this: Spot Option was accused by the SEC of designing its platform to increase the probability of investor losses [20], while the operators of Yukom/BinaryBook allegedly manipulated risk settings to limit winning trades [29], and the Cartu operation allegedly manipulated trade results directly.[31] Because these unregulated platforms often act as the direct counterparty to every client trade [20]—meaning the platform wins when the client loses, and vice versa [21]—there is a direct financial incentive to ensure clients fail. The "trading" becomes a simulation designed solely to extract funds.

- **Refusal to Credit Accounts or Process Withdrawals:** A very common complaint involves the inability of customers to access their funds.[4] Platforms readily accept deposits, often encouraging larger and repeated investments through persuasive "brokers".[9] However, when customers attempt to withdraw their initial deposit or any purported profits, they face insurmountable obstacles.[4] Withdrawal requests may be outright cancelled, ignored, or endlessly delayed with excuses about processing or documentation requirements.[17] Customer service lines go unanswered, emails are ignored, and in some cases, accounts are frozen, sometimes with the platform accusing the *customer* of fraud.[4] Spot Option allegedly instructed its partners to limit withdrawals deliberately [20], and operators like Yukom and Cartu used tactics like deceptive bonus conditions specifically to prevent funds from being withdrawn.[30] This ensures that money flows only one way – into the scam.
- **Identity Theft and Misuse of Personal Information:** Beyond stealing deposited funds, many fraudulent platforms engage in identity theft.[4] They often request extensive personal documentation—such as copies of credit cards (front and back), passports, driver's licenses, and utility bills—under the guise of regulatory compliance or account verification.[4] While legitimate financial institutions require identity verification, unregulated scammers collect far more data than necessary [9] and misuse it.[12] This sensitive information can then be used to open other fraudulent accounts, commit further financial crimes in the victim's name, or be sold on the dark web.[4] This tactic adds a significant layer of long-term harm for the victim, extending far beyond the initial investment loss.
- **Aggressive Sales Tactics and Fake Brokers:** Binary options scams heavily rely on psychological manipulation through high-pressure sales tactics, often originating from "boiler room" call centers.[13] Individuals posing as experienced "brokers," "traders," or "account managers" contact potential victims, often unsolicited.[13] These individuals typically use fake names and credentials, misrepresent their location (claiming to be in major financial centers when often operating from offshore call centers), and lie about their expertise and track record.[21] They build a false sense of trust and rapport, encouraging initial small deposits and then relentlessly pressuring for larger sums, often using fabricated success stories or time-limited opportunities.[13] The case of Yukom/BinaryBook revealed CEO Lee Elbaz explicitly fostering a high-pressure "boiler room" environment.[21] The Cartu scheme also involved brokers misrepresenting their identities and expertise.[31] This fabricated relationship is designed solely to extract as much money as possible before the victim realizes they are being defrauded.
- **Misleading "Bonuses" and "Risk-Free" Trades:** To entice deposits and lock in funds, scam platforms frequently offer seemingly attractive bonuses (e.g.,

matching a deposit) or "risk-free" trades.[17] However, these offers invariably come with hidden, complex, or unattainable conditions.[17] Typically, accepting a bonus requires the trader to achieve an extremely high trading volume before *any* funds (including the original deposit) can be withdrawn.[17] These volume requirements are often set so high that they are practically impossible to meet without losing the entire account balance. "Risk-free" trades might refund a loss as bonus credit, subject to the same restrictive withdrawal conditions. Evidence from the Cartu case showed that bonuses were explicitly used internally as a tool to prevent withdrawals and thus increase the platform's profits.[35] Similarly, Yukom/BinaryBook representatives misrepresented the terms of these offers.[38] These are not genuine benefits but carefully constructed traps designed to prevent investors from ever accessing their money.[21]

3. Red Flags: Identifying Potential Binary Options Scams

Given the prevalence of fraud, potential investors must be vigilant and learn to recognize the common warning signs associated with binary options scams. The presence of one or more of these red flags should prompt extreme caution.

3.1. Guaranteed High Returns and Unrealistic Promises

A classic hallmark of investment fraud is the promise of unusually high, guaranteed, or quick returns with little or no associated risk.[4] Fraudulent binary options platforms often advertise returns of 60%, 85%, or even higher within very short timeframes, suggesting easy profits.[12] Legitimate financial markets operate on the principle that higher potential returns invariably come with higher risk; guarantees of high returns are almost always fictitious.[16] Such promises are designed to appeal to greed and bypass rational assessment of the investment's viability.

3.2. High-Pressure Sales Tactics

Scammers frequently employ aggressive and persistent sales tactics to rush potential victims into making deposits before they have time for proper research or reflection.[13] This can manifest as repeated unsolicited phone calls or emails, the creation of artificial urgency (e.g., "This opportunity is only available today!"), threats of missed opportunities, or overly familiar and pushy "brokers".[13] Legitimate investment firms provide information and allow clients adequate time to make considered decisions. Intense pressure to invest immediately is a significant red flag.

3.3. Issues with Fund Withdrawals

While this often becomes apparent only after funds have been deposited, difficulty in accessing or withdrawing money is a critical indicator of a scam.[9] Victims report that withdrawal requests are ignored, endlessly delayed with flimsy excuses, subjected to sudden new fees or documentation requirements, or outright refused.[4] Platforms may become unresponsive once a withdrawal is requested. Since the primary goal of these scams is to steal funds, any impediment to retrieving deposited money should be treated as a serious warning sign.

3.4. Unsolicited Contact

Receiving unexpected contact—whether through cold calls, emails, social media messages, or pop-up online advertisements—promoting binary options trading is highly suspicious.[4] Reputable financial institutions generally do not solicit new clients through such aggressive, unsolicited methods. These contacts often originate from boiler rooms or marketing campaigns specifically designed to find potential victims.

3.5. Lack of Verifiable Registration or Licensing

This is a crucial check. Legitimate financial services providers operating in regulated markets (like the US, UK, EU, Australia) are required to be registered or authorized by the relevant financial regulatory authority.[13] Fraudulent platforms often operate without registration, falsely claim to be regulated, or are based in jurisdictions with weak or non-existent oversight.[17] Before engaging with any platform, investors should independently verify its registration status using the official online tools provided by regulators like the SEC, CFTC, FCA, ESMA/NCAs, ASIC, NFA, or FINRA.[9] An inability to find the platform or its representatives listed on these official registers is a strong indication of illegitimacy.

3.6. Table: Warning Signs Checklist

Potential investors can use the following checklist to assess a binary options provider. The more "Yes" answers, the higher the likelihood of encountering a scam:

Warning Sign	Check (Yes/No/Unsure)	Notes
Promises of Guaranteed High/Quick Returns?		Legitimate investments involve risk; high returns are never guaranteed.
High-Pressure Sales Tactics Used?		Urgency, excessive calls, pressure to deposit immediately.

Reported Issues with Fund Withdrawals?		Check online reviews/forums (cautiously), test with small withdrawal.
Was Contact Unsolicited (Cold Call, Email, Ad)?		Reputable firms rarely use aggressive cold outreach.
Registration/License Unverifiable with Regulator?		Check official regulator websites (SEC, CFTC, FCA, ASIC, etc.).
Requests for Excessive Personal Data?		Photocopies of credit cards, excessive ID beyond basic KYC.
Terms & Conditions Vague, Complex, or Unfair?		Especially regarding bonuses and withdrawals.
Platform Based Offshore / In Unregulated Location?		Significantly increases risk and limits recourse.

4. Regulatory Warnings and Actions

Financial regulators across the globe have recognized the significant threat posed by binary options fraud and have taken various actions, ranging from issuing public warnings to implementing outright bans and pursuing enforcement actions against fraudulent operators.

4.1. Stance of U.S. Regulators (SEC & CFTC)

In the United States, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) share oversight depending on the underlying asset of the binary option (securities for SEC, commodities/forex/indices for CFTC).[9] Both agencies have issued numerous joint Investor Alerts explicitly warning the public about fraudulent binary options schemes.[9] These alerts highlight common scam tactics such as operating unregistered platforms, refusing to pay out funds, committing identity theft, and manipulating trading software.[23]

U.S. regulators emphasize that for binary options to be legally offered to retail customers in the U.S., they must generally be traded on an exchange registered with the SEC or a Designated Contract Market (DCM) registered with the CFTC.[4] They consistently point out that only a very small number of such regulated venues exist (Nadex being the primary example for CFTC-regulated options).[4] Any other entity soliciting U.S. customers for binary options trading, especially those based online and offshore, is likely operating illegally.[9]

To aid investors, the CFTC maintains a Registration Deficient (RED) List identifying foreign entities believed to be soliciting U.S. residents without proper registration.[4] Both agencies provide online tools (like EDGAR, NFA BASIC, FINRA BrokerCheck) for investors to verify the registration status of platforms and individuals.[4]

Furthermore, the SEC and CFTC actively pursue enforcement actions against fraudulent binary options operators targeting U.S. investors, seeking court orders for injunctions, disgorgement of illicit profits, and civil monetary penalties, as seen in the cases against Spot Option, Yukom, and Cartu.[20] While acknowledging the existence of a small, regulated market, the overwhelming message from U.S. regulators is one of extreme caution due to the prevalence of illegal and fraudulent activity in the broader binary options space accessible online.

4.2. Stance of UK Regulator (FCA) - Including Ban

The UK's Financial Conduct Authority (FCA) adopted a decisive stance against binary options. Citing significant consumer harm, the inherent risks associated with the product (viewing it akin to fixed-odds betting), and its complexity, the FCA implemented a ban on the sale, marketing, and distribution of binary options to all retail consumers in the UK.[22] This ban took effect on April 2, 2019.[22]

Consequently, the FCA warns that any firm currently offering binary options services to retail clients within the UK is highly likely to be operating without authorization or is an outright scam.[22] The regulator strongly advises consumers to deal only with FCA-authorised firms and to verify any firm's status and permissions using the official Financial Services Register before engaging with them.[22] The UK's approach reflects a judgment that the product itself poses unacceptable risks to retail investors, leading to a complete prohibition rather than allowing a regulated market segment for retail participants.

4.3. Stance of EU Regulator (ESMA) - Including Ban

The European Securities and Markets Authority (ESMA), the EU's overarching securities markets regulator, addressed binary options fraud on a pan-European level. Recognizing significant investor protection concerns stemming from the products' complexity, lack of transparency, negative expected returns for investors, and inherent conflicts of interest in their distribution, ESMA utilized its product intervention powers under the Markets in Financial Instruments Regulation (MiFIR).[40]

Starting on July 2, 2018, ESMA implemented temporary EU-wide measures prohibiting the marketing, distribution, or sale of binary options to retail clients.[3] These temporary measures were renewed several times.[44] Certain very specific types of binary options, structured to mitigate risk (e.g., fully collateralized, long-term, prospectus-backed, no provider market risk), were later excluded from the renewed prohibitions.[40]

ESMA ultimately ceased renewing the temporary EU-wide ban on July 1, 2019.[46] This decision was made because, by that time, a majority of the National Competent Authorities (NCAs) – the individual financial regulators within each EU member state – had adopted their own permanent national product intervention measures regarding binary options.[46] These national measures were generally at least as stringent as ESMA's temporary ban, effectively making the EU-wide measure redundant but ensuring continued protection at the national level across most of the EU.[43] This coordinated approach, initiated by ESMA and finalized by NCAs, demonstrates a strong consensus across the European Union regarding the dangers binary options pose to retail investors.

4.4. Stance of Australian Regulator (ASIC) - Including Ban

The Australian Securities and Investments Commission (ASIC) took a similar path to the UK and EU regulators. Following initial warnings and reviews that revealed alarmingly high loss rates among retail clients (around 80% losing money) [48], ASIC determined that binary options were causing significant detriment.[48] ASIC's analysis found substantial aggregate net losses for retail clients trading these products—$14 million in the 13 months preceding the ban.[49]

Using its product intervention powers, ASIC implemented an order banning the issue and distribution of binary options to retail clients, effective from May 3, 2021.[3] This ban was subsequently reviewed, and its effectiveness in preventing further retail client losses was confirmed.[50] Consequently, ASIC extended the ban significantly, ensuring it remains in effect until at least October 1, 2031.[49] This long-term ban reflects Australia's firm regulatory stance against offering these high-risk products to retail investors.

4.5. Table: Summary of Regulatory Actions/Bans

The following table summarizes the regulatory positions and key actions taken in major jurisdictions regarding binary options for retail clients:

Jurisdiction	Regulator(s)	Key Action	Status / Effective Date	Key Snippets
USA	SEC & CFTC	Warnings; Enforcement; Requires Exchange Trading	Ongoing; Limited Legal Venues	[4]
UK	FCA	Ban on Retail Sale, Marketing, Distribution	Banned since April 2, 2019	[22]
EU	ESMA & NCAs	Initial ESMA Ban; Now Permanent National Bans	Banned via National Measures	[40]
Australia	ASIC	Ban on Retail Issue and Distribution	Banned since May 3, 2021 (Extended to 2031)	[48]

The consistent pattern across these major regulatory bodies underscores the global recognition of the severe risks and fraudulent potential associated with binary options when offered to retail investors, leading most major jurisdictions outside the US to implement outright bans.

5. Case Studies: Binary Options Scams in Action

Examining specific enforcement actions provides concrete examples of how binary options scams operate, the scale they can reach, and the tactics regulators actively combat.

5.1. Spot Option / Pini Peter Case (Platform Provider)

The case against Spot Tech House Ltd. (formerly Spot Option Ltd.) and its key executives highlights the crucial role played by technology providers in enabling widespread binary options fraud.[20] Spot Option, based in Israel, did not typically deal directly with retail investors. Instead, it developed and licensed a comprehensive binary options trading platform and associated services to numerous other entities worldwide, referred to as "white label partners".[20]

The SEC alleged that Spot Option, under the direction of its founder/CEO Malhaz

Patarkazishvili (also known as Pini Peter) and president Ran Amiran, was central to a scheme that defrauded U.S. investors of over $100 million.[20] The allegations stated that Spot Option actively instructed its white label partners on how to conduct fraudulent operations. This included advising partners to aggressively market binary options as highly profitable investments while concealing the fact that the partners (and thus Spot Option indirectly) acted as the counterparty on all trades, profiting directly from investor losses.[20]

Crucially, Spot Option was accused of designing its platform and instructing partners to implement specific manipulative tactics to ensure investor losses and maximize profits. These tactics allegedly included: allowing investors to withdraw only a portion of their deposited funds, devising a manipulative payout structure for trades, and designing the trading platform itself to increase the probability that trades would expire worthless (out-of-the-money).[20]

The SEC charged Spot Option and its executives with fraud and registration violations, seeking significant financial penalties, disgorgement of ill-gotten gains, and permanent injunctions.[20] Subsequent court actions resulted in substantial monetary judgments against the company and Pini Peter, although these decisions have faced appeals.[26] This case demonstrates that regulatory scrutiny extends beyond the frontline brokers to the underlying technology providers who facilitate and potentially orchestrate large-scale fraud.

5.2. Yukom Communications / BinaryBook / Lee Elbaz Case (Operator)

The Yukom Communications case provides a stark example of a large, centrally organized fraudulent binary options operation.[39] This Israeli-based enterprise operated multiple outwardly distinct but internally connected brands, including BinaryBook, BigOption, and BinaryOnline, targeting investors globally, including significant numbers in the United States.[21]

The CFTC and Department of Justice alleged a massive fraud, with the enterprise soliciting and accepting over $103 million (and potentially up to $145 million according to DOJ figures) from victims.[21] The core of the fraud involved systematic misrepresentation and manipulation. Yukom's "brokers" (sales agents), under the leadership of CEO Lee Elbaz, allegedly lied about their identities, locations, expertise, and the nature of the binary options being offered.[21] They falsely claimed the trades were legitimate market transactions and profitable opportunities, when in reality, the vast majority of customers (estimated at 95%) lost money.[21]

The enterprise acted as the counterparty, directly benefiting from these losses.[21]

Evidence suggested the platform's risk settings were manipulated to disadvantage clients [29], and deceptive tactics like misleading bonus offers and "risk-free" trades were used to encourage deposits and prevent withdrawals.[21] CEO Lee Elbaz was documented encouraging a high-pressure "boiler room" sales environment.[21]

The consequences were severe. The CFTC obtained a default judgment ordering the Yukom entities and key individuals (including Yossi Herzog, Lee Elbaz, Shalom Peretz, and Yakov Cohen) to pay over $451 million in restitution and penalties.[29] In a parallel criminal case, Lee Elbaz was convicted by a U.S. jury of wire fraud and conspiracy and sentenced to 20 years in prison, with a $28 million restitution order.[21] Several other individuals involved also faced criminal charges and settled with the CFTC.[39] The Yukom case exemplifies the coordinated use of civil regulatory action and criminal prosecution to dismantle a major international fraud operation.

5.3. Jonathan Cartu / Blue Moon Investments Case (Operator)

This case illustrates the use of complex corporate structures and interconnected entities to perpetrate and conceal a large-scale binary options fraud.[31] The scheme allegedly involved Canadian brothers Jonathan, David, and Joshua Cartu, along with Israeli brothers Leeav and Nati Peretz.[35] They operated fraudulent binary options brands including BeeOptions, Glenridge Capital, and Rumelia Capital, primarily targeting U.S. residents through call centers located mainly in Israel.[31]

The CFTC alleged that these individuals and their associated companies, including offshore entities like Blue Moon Investments (controlled by Jonathan Cartu and registered in the Seychelles), offered illegal, off-exchange binary options.[32] The operation involved numerous material misrepresentations typical of such scams: promises of quick, high returns (60-85%), false claims that the company's interests aligned with customers', and misrepresentations about brokers' expertise and identity.[31]

A key aspect was the control over the entire process. The Cartus, allegedly in concert with Ryan Masten and his Texas company BareIt Media, developed and operated their own internet-based trading platform used by their brands and potentially others.[31] This allowed them to control the transactions and allegedly manipulate trade results to force customer losses.[32] Furthermore, the Cartu brothers operated Greymountain Management Limited, an Irish-based payment processor, which facilitated the transfer of over $165 million in customer funds, primarily via credit card payments, effectively laundering the proceeds of the fraud.[31] Deceptive bonuses were also used as a tool to prevent customer withdrawals.[35]

The CFTC filed suit, and despite initial difficulties locating and serving some of the offshore defendants [61], ultimately secured a default judgment against Jonathan Cartu, the Peretz brothers, and Blue Moon Investments.[32] The court found them liable for fraud and illegal options offering, ordering them to pay over $204 million ($51.1M in disgorgement and $153.5M in penalties) and imposing permanent trading and registration bans.[28] This case highlights the intricate web of offshore companies, proprietary platforms, and payment processors used to sustain such fraudulent enterprises.

6. The High Cost: Financial Risks and Potential Losses

Engaging with binary options, particularly through unregulated platforms, exposes individuals to substantial financial risks far exceeding those associated with conventional, regulated investments. The potential for significant, often total, loss is exceptionally high due to both the inherent structure of the product and the prevalence of outright fraud.

6.1. Inherent Risk: The All-or-Nothing Gamble

The fundamental design of a binary option involves a stark, binary outcome: the trader either receives a predetermined fixed payout if their prediction is correct at expiration, or they lose their entire initial investment (the premium paid for the option) if they are wrong.[1] There is typically no partial recovery on a losing trade, unlike holding a stock that declines in value but still retains some worth.[3] While some platforms might allow closing a position before expiration, this often results in accepting a reduced profit or locking in a partial loss.[3]

This all-or-nothing structure, combined with the often extremely short timeframes (minutes or hours) involved, leads many observers and regulators to compare binary options trading to gambling rather than investing.[3] Predicting precise, short-term price movements is inherently speculative and difficult [11], making the activity more akin to placing a bet on a future event than making an informed investment decision based on fundamental value or long-term trends.[3] Even when traded legitimately, the high degree of speculation makes binary options unsuitable for most individuals' investment objectives.

6.2. Negative Expected Returns and the House Edge

Beyond the basic all-or-nothing risk, the typical payout structure of binary options is often mathematically disadvantageous to the trader.[3] When an option expires in the money, the payout received is usually less than 100% of the amount risked. For example, a $100 investment might yield a profit of $70 to $85 (a total return of

$170-$185) if successful.[3] However, if the trade is unsuccessful, the loss is 100% of the $100 invested.[11]

This asymmetry means that a trader needs to win significantly more often than they lose just to break even.[3] If the odds of predicting the price movement correctly are roughly 50/50 (a reasonable assumption for very short-term, random fluctuations), this payout structure guarantees a negative expected return over time.[9] The platform, whether legitimate or fraudulent, holds a statistical "house edge".[3] Fraudulent platforms can further exacerbate this disadvantage through manipulated pricing or outcomes.[16] This built-in structural bias, often obscured by aggressive marketing promising easy profits, makes sustained profitability extremely challenging for retail traders.

6.3. Potential for Total Loss of Investment

The combination of the all-or-nothing structure, the negative expected return, and the prevalence of fraudulent practices makes the risk of losing the entire amount invested in binary options exceptionally high.[2] On fraudulent platforms designed to ensure customer failure through manipulated software [4] and that actively prevent withdrawals [4], the loss of all deposited funds is not just a risk, but the likely and intended outcome. Victims are often encouraged to make repeated deposits, chasing losses or believing false promises of recovery, only to find their entire capital inaccessible and ultimately gone.[9] This represents the devastating financial consequence for individuals ensnared in these schemes – the complete evaporation of their funds.

6.4. The Scale of the Problem: Estimated Global Losses

The cumulative financial damage caused by binary options fraud is staggering. As previously noted, the FBI has estimated annual worldwide losses attributable to these scams at around US$10 billion.[3] While precise figures are difficult to ascertain due to underreporting and the cross-jurisdictional nature of the crime, available data points to a massive problem.

The FBI's IC3 reporting data showed a rapid escalation in the mid-2010s, with reported losses climbing into the millions annually in the US alone, representing only the tip of the iceberg.[4] Reports from some European nations indicated binary options fraud constituted a significant portion (up to 25%) of all fraud complaints during that period.[27]

Furthermore, the scale of individual enforcement actions provides insight into the amounts involved. The Yukom/BinaryBook operation handled over $100 million [30], and the Cartu enterprise processed over $165 million through its payment channels.[31] These figures demonstrate that binary options fraud is not a minor issue but a major international financial crime causing billions in losses to potentially millions of victims globally, necessitating robust awareness campaigns and continued regulatory vigilance.

7. Protecting Yourself: Verification and Due Diligence

Given the high prevalence of fraud in the binary options market, particularly online, rigorous due diligence and verification are paramount before considering any engagement. Taking proactive steps to check the legitimacy of a platform is the most effective way to avoid becoming a victim.

7.1. Verifying Platform Legitimacy (Registration Checks)

The single most important step before depositing any funds or providing personal information is to verify the registration and licensing status of the binary options platform and any associated individuals (like "brokers" or account managers).[4] Legitimate financial service providers are required to be registered with the appropriate regulatory bodies in the jurisdictions where they operate or solicit clients.[13] Scammers often falsely claim registration or operate entirely outside the regulatory system.[17] Investors should *independently* verify any claims using official regulator resources:

- **In the United States:**
  - Check if the specific binary option *product* offering is registered with the **SEC** using the **EDGAR** database.[4]
  - Check if the *platform* is registered as an exchange with the **SEC** via their **Exchanges list**.[4]
  - Check if the *platform* is registered as a Designated Contract Market (DCM) with the **CFTC** using their **DCM list** (especially critical for options on commodities, forex, indices).[4] Remember, only a few DCMs are authorized for binary options.[18]
  - Consult the **CFTC's RED List** for known unregistered foreign entities soliciting US residents.[4]
  - Use the **National Futures Association (NFA) BASIC Database** to check the registration status and disciplinary history of firms and individuals in the derivatives/futures industry.[4]
  - Use **FINRA's BrokerCheck** tool to verify the registration and background of broker-dealers and associated individuals.[4]

- **In the United Kingdom:**
  - Check the **FCA's Financial Services Register** to confirm if a firm is authorised by the FCA and has the necessary permissions for the services offered.[22] Given the ban, finding a firm authorized for retail binary options is highly unlikely.
- **In the European Union:**
  - Contact the **National Competent Authority (NCA)** in the relevant EU member state (usually the national financial regulator or central bank). ESMA generally directs inquiries to the NCAs.[63] Due to national bans, legitimate retail offerings are rare.
- **In Australia:**
  - Use **ASIC's Professional Registers** to check if a company or individual holds an Australian Financial Services (AFS) licence or is an authorised representative.[65]
  - Check **ASIC's Banned and Disqualified Register**.[65] Again, the retail ban makes legitimate offerings virtually non-existent.

Crucially, if a platform or individual cannot be verified through these official channels, or if they appear on a warning list like the RED List, they should be avoided entirely. Do not rely on registration claims made by the platform itself; always conduct independent verification.[17]

7.2. Avoiding Unregulated and Offshore Platforms

Given that much of the fraud originates from platforms operating outside established regulatory frameworks, particularly those based in offshore jurisdictions, a prudent approach is to avoid them altogether.[2] Dealing with such entities carries immense risk, as investors lose the legal and regulatory protections available in well-regulated markets.[14] Recourse in case of disputes or fraud is minimal to non-existent. Furthermore, it is often illegal for these offshore platforms to solicit customers in regulated jurisdictions like the US, UK, EU, or Australia without proper registration.[9] The potential allure of easy profits advertised by these platforms is vastly outweighed by the high probability of encountering fraud and losing invested capital.

7.3. Understanding the Investment Before Committing Funds

A fundamental principle of investor protection is to never invest in something one does not fully understand.[4] Binary options, despite their superficial simplicity, involve complex underlying probabilities and payout structures that are often disadvantageous.[3] Potential investors should demand clear explanations of how the platform works, how prices are determined, the exact payout structure, associated fees, and the specific risks involved. If a platform representative ("broker") cannot provide clear, understandable answers or resorts to jargon and pressure tactics, it is a major warning sign.[34] Conducting independent research beyond the platform's marketing materials is essential to gain an objective understanding.[65]

7.4. Protecting Personal Information

Fraudulent binary options platforms often seek excessive personal information under the guise of account setup or verification.[4] Be extremely cautious about providing copies of sensitive documents like credit cards (front and back), passports, driver's licenses, or utility bills.[4] Before sharing any personal data, ensure the platform has been verified as legitimate and regulated through official channels.[9] Understand why the information is being requested and provide only what is necessary for standard Know Your Customer (KYC) procedures with a verified entity. Sharing excessive data with unverified or fraudulent platforms significantly increases the risk of identity theft, compounding potential financial losses.[4]

8. Seeking Recourse: Reporting Fraud and Getting Assistance

Discovering you have been victimized by a binary options scam can be devastating. While recovering lost funds is often difficult, especially from offshore entities, reporting the fraud promptly is crucial for potential law enforcement action, regulatory intervention, and preventing others from falling victim.

8.1. Immediate Steps for Victims

If you suspect you have been scammed:

1. **Cease All Contact:** Immediately stop all communication with the fraudulent platform and its representatives. Do not respond to further calls, emails, or messages.[22] Block their numbers and email addresses.
2. **Contact Your Financial Institution(s):** Notify your bank, credit card company, or any payment processor used immediately. Report the transactions as fraudulent and request that they stop any pending payments or attempt to reverse charges (chargebacks may be possible for credit card payments within certain timeframes).[66]
3. **Gather Evidence:** Collect and preserve all records related to the scam. This includes website addresses, names and contact details used by "brokers," copies of emails, chat logs, transaction records, account statements, and any promotional materials.[66]
4. **Beware of Recovery Scams:** Be extremely wary of unsolicited offers from individuals or companies claiming they can recover your lost funds, usually for an

upfront fee.[13] These are often secondary scams run by the original fraudsters or their associates, designed to extract even more money from victims. Legitimate recovery efforts typically occur through official regulatory or legal channels, not through unsolicited offers demanding payment.

8.2. Reporting Channels in the US

- **Commodity Futures Trading Commission (CFTC):** If the scam involved binary options based on commodities, forex, or indices, report it to the CFTC.
  - Online Tip/Complaint Form: Available on CFTC.gov.[9]
  - Toll-Free Hotline: 866-FON-CFTC (866-366-2382).[58]
  - Whistleblower Program: For individuals with inside information.[9]
- **Securities and Exchange Commission (SEC):** If the scam involved binary options based on stocks or securities, or if unsure, report to the SEC.
  - Online Complaint Portal (TCR System): Accessible via SEC.gov or Investor.gov.[18]
  - Investor Assistance Line: (800) 732-0330.[18]
- **Federal Bureau of Investigation (FBI):** Report the crime to the FBI, particularly for potential criminal investigation.
  - Internet Crime Complaint Center (IC3): IC3.gov.[4]
  - Local FBI Field Office: Contact details available on FBI.gov.[71]
- **National Futures Association (NFA):** If the firm or individual involved was potentially an NFA member, a complaint can be filed.[9] (Website: NFA.futures.org).

8.3. Reporting Channels in the UK

- **Financial Conduct Authority (FCA):** Report suspected scams, unauthorized firms, or misleading promotions directly to the FCA.
  - Phone: 0800 111 6768.[22]
  - Online Contact Form: Available on FCA.org.uk.[22]
- **Action Fraud:** The UK's national reporting centre for fraud and cybercrime, which passes reports to the police for investigation.
  - Website: ActionFraud.police.uk.[22]

8.4. Reporting Channels in the EU

- **National Competent Authorities (NCAs):** The primary point of contact for reporting investment fraud is typically the financial regulator in the victim's own EU member state, or the state where the firm claimed to operate.[63] Contact details can usually be found on the website of the national central bank or financial supervisory authority.
- **European Securities and Markets Authority (ESMA):** ESMA does *not* handle

individual consumer complaints or fraud cases.[63] However, you can contact them at scamreport@esma.europa.eu if you suspect misuse of ESMA's name or logo.[63] Breaches of Union law by NCAs or certain supervised entities can be reported through specific channels (e.g., whistleblower platform).[73]
- **Local Law Enforcement:** Report the crime to your local police department.[63]
- **European Anti-Fraud Office (OLAF):** Only relevant if the fraud involves misuse of EU public funds or serious misconduct by EU officials, not typical retail investment scams.[75]

8.5. Reporting Channels in Australia

- **Australian Securities and Investments Commission (ASIC):** Report misconduct related to financial products, investment scams, or companies impersonating legitimate firms.[67] (Website: ASIC.gov.au, Moneysmart.gov.au).
- **Scamwatch:** Run by the National Anti-Scam Centre, this is a primary reporting point for all types of scams. Reports help warn the public and inform relevant agencies.[66] (Website: Scamwatch.gov.au).
- **ReportCyber (Australian Cyber Security Centre - ACSC):** Report cybercrimes, especially if personal information or online accounts were compromised.[66] (Website: Cyber.gov.au).
- **IDCARE:** A free, government-funded service providing support to victims of identity theft and cybercrime.[66] (Website: IDCARE.org).
- **Local Police:** Report the fraud as a crime to your state or territory police.[67]

8.6. Table: Key Reporting Resources by Jurisdiction

This table provides a quick reference for key resources in major jurisdictions:

Jurisdiction	Purpose	Agency/Resource	Website / Contact
USA	Verify Registration	CFTC DCM List, SEC EDGAR/Exchanges, NFA BASIC, FINRA BrokerCheck	CFTC.gov, SEC.gov, NFA.futures.org, FINRA.org
	Report Fraud (Commodities)	CFTC	CFTC.gov (Online Tip Form / Hotline)
	Report Fraud (Securities)	SEC	SEC.gov / Investor.gov (Online Complaint)

	Report Crime	FBI (IC3)	IC3.gov
UK	Verify Authorisation	FCA Financial Services Register	register.fca.org.uk
	Report Fraud (Regulator)	FCA	FCA.org.uk (Online Form / Hotline)
	Report Crime	Action Fraud	ActionFraud.police.uk
EU	Verify Registration	National Competent Authority (NCA)	Varies by country (check national regulator site)
	Report Fraud	National Competent Authority (NCA)	Varies by country
	Report Crime	Local Police	Local police contact
Australia	Verify Licence	ASIC Professional Registers	ASIC.gov.au / connectonline.asic.gov.au
	Report Scams (Central)	Scamwatch	Scamwatch.gov.au
	Report Financial Misconduct	ASIC	ASIC.gov.au / Moneysmart.gov.au
	Report Cybercrime	ReportCyber (ACSC)	Cyber.gov.au
	Get Support	IDCARE	IDCARE.org

Conclusion

Binary options fraud represents a significant and persistent threat to investors worldwide. While a small, regulated market for these instruments exists in some jurisdictions like the US, the overwhelming majority of binary options activity accessible online occurs through unregulated, often offshore platforms that frequently engage in fraudulent practices. The simplicity of the binary option's "yes/no" structure is deceptively appealing, masking inherent statistical disadvantages for traders and providing fertile ground for scams.

Fraudulent operators employ a consistent set of tactics, including manipulating trading software to ensure client losses, refusing to process withdrawals, using high-pressure sales tactics through fake brokers, offering misleading bonuses to trap funds, and stealing personal information for identity theft. The scale of the problem is vast, with estimated global losses running into billions of dollars annually, facilitated by the ease of setting up online platforms and the challenges of cross-border enforcement.

Regulatory bodies across major financial centers have responded decisively. The US SEC and CFTC issue frequent warnings and pursue enforcement actions, emphasizing the need to use only registered domestic exchanges. The UK's FCA, the EU's ESMA (leading to national actions), and Australia's ASIC have gone further, implementing outright bans on the sale of binary options to retail clients due to the profound risks and documented harm.

Protecting oneself requires unwavering vigilance and skepticism. Promises of guaranteed high returns, unsolicited offers, and pressure to invest quickly are major red flags. The most critical protective measure is rigorous due diligence, primarily verifying the registration and regulatory status of any platform and associated individuals through official channels before committing any funds or personal data. Avoiding unregulated and offshore platforms entirely is often the safest course of action.

For those who fall victim, immediate reporting to financial institutions and relevant regulatory and law enforcement agencies is essential, although recovery of lost funds remains challenging. Awareness of the common scam tactics, adherence to due diligence practices, and reliance on verified, regulated entities are the cornerstones of safeguarding investments against the pervasive threat of binary options fraud.

Works cited

1. www.investopedia.com, accessed on April 18, 2025, https://www.investopedia.com/articles/active-trading/061114/guide-trading-binary-options-us.asp#:~:text=Binary%20options%20are%20based%20on,which%20option%20is%20more%20likely.
2. Binary Option: Definition, How They Trade, and Example - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/terms/b/binary-option.asp
3. Binary option - Wikipedia, accessed on April 18, 2025, https://en.wikipedia.org/wiki/Binary_option

4. Binary Options Fraud - FBI, accessed on April 18, 2025, https://www.fbi.gov/news/stories/binary-options-fraud
5. The Most Important Technical Indicators for Binary Options - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/articles/active-trading/022615/most-important-technical-indicators-binary-options.asp
6. A Guide to Trading Binary Options in the US - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/articles/active-trading/061114/guide-trading-binary-options-us.asp
7. Binary Options Strategies You Should Know - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/articles/active-trading/052014/binary-options-strategies.asp
8. Trading Binary Options: The Basics - YouTube, accessed on April 18, 2025, https://www.youtube.com/watch?v=Pr3qCKn-2UI
9. CFTC/SEC Investor Alert: Binary Options and Fraud | CFTC, accessed on April 18, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/fraudadv_binaryoptions.html
10. What are Binary Options and How Do They Work? - Nadex, accessed on April 18, 2025, https://www.nadex.com/learning/what-are-binary-options-and-how-do-they-work/
11. Currency Binary: What It is, How it Works, Examples - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/terms/c/currency-binary.asp
12. The Basics of Investing In Binary Options - Washington State Department of Financial Institutions, accessed on April 18, 2025, https://dfi.wa.gov/financial-education/information/basics-investing-binary-options
13. Beware of Online Binary Options Schemes - Missouri Secretary of State, accessed on April 18, 2025, https://www.sos.mo.gov/bewareofonlinebinaryoptionsschemes
14. Are binary options legal in the US? - Nadex, accessed on April 18, 2025, https://www.nadex.com/blog/are-binary-options-legal-in-the-us/
15. Trading Forex With Binary Options - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/articles/forex/022415/trading-forex-binary-options.asp
16. Binary Options Fraud | Investor.gov, accessed on April 18, 2025, https://www.investor.gov/protect-your-investments/fraud/types-fraud/binary-options-fraud
17. Beware of Off-Exchange Binary Options Trades | CFTC, accessed on April 18, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/beware_of_off_exchange_binary_options.htm

18. Investor Alert: Binary options and Fraud - SEC.gov, accessed on April 18, 2025, https://www.sec.gov/investor/alerts/ia_binary.pdf
19. How to Hedge Stock Positions Using Binary Options - Investopedia, accessed on April 18, 2025, https://www.investopedia.com/articles/active-trading/073015/how-hedge-stock-positions-using-binary-options.asp
20. SEC Charges Binary Options Trading Platform and Two ... - SEC.gov, accessed on April 18, 2025, https://www.sec.gov/newsroom/press-releases/2021-66
21. CFTC Charges International Enterprise with Operating a $103 Million Fraudulent Binary Options Trading Scheme, accessed on April 18, 2025, https://www.cftc.gov/PressRoom/PressReleases/7995-19
22. Binary options scams | FCA, accessed on April 18, 2025, https://www.fca.org.uk/consumers/binary-options-scams
23. Binary Options Fraud | CFTC, accessed on April 18, 2025, https://www.cftc.gov/BinaryOptionsFraud/index.htm
24. Beware the Binary Options Scam | Blockchain Intelligence Reveals Network of Vietnamese Operators - TRM Labs, accessed on April 18, 2025, https://www.trmlabs.com/post/beware-the-binary-options-scam
25. RMG 2021 Impact Report *FINAL DRAFT* - Reink Media Group, accessed on April 18, 2025, https://www.reinkmedia.com/wp-content/uploads/2022/03/RMG-2021-Impact-Report-_FINAL-DRAFT_.pdf
26. Binary Options Fraud - MarketsWiki, A Commonwealth of Market Knowledge, accessed on April 18, 2025, https://www.marketswiki.com/wiki/Binary_Options_Fraud
27. FBI places public warning against 'Binary Options Fraud' at top of its main website, accessed on April 18, 2025, https://www.timesofisrael.com/fbi-places-public-warning-against-binary-options-fraud-at-top-of-its-main-website/
28. Federal Court Orders Binary Options Firm and Owners to Pay Over $204 Million in Monetary Sanctions for Fraudulent Binary Options, accessed on April 18, 2025, https://business.cch.com/srd/8877-24.pdf
29. Binary options fraudsters ordered to pay US$450 million - Investment Executive, accessed on April 18, 2025, https://www.investmentexecutive.com/news/from-the-regulators/binary-options-fraudsters-ordered-to-pay-us450-million/
30. UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS COMMODITY FUTURES TRADING COMMISSION, Plaintiff, v. YUKOM C, accessed on April 18, 2025, https://www.cftc.gov/media/2331/enfyukombinaryperetzcomplaint08122019/download
31. Commodity Futures Trading Comm'n v. Cartu, 1:20-CV-908-RP | Casetext Search + Citator, accessed on April 18, 2025, https://casetext.com/case/commodity-futures-trading-commn-v-cartu-1
32. Federal Court Orders Binary Options Firm and Owners to Pay Over $204 Million in

Monetary Sanctions for Fraudulent Binary Options Scheme | CFTC, accessed on April 18, 2025, https://www.cftc.gov/PressRoom/PressReleases/8877-24
33. 1 IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TEXAS AUSTIN DIVISION COMMODITY FUTURES TRADING § COMMISSION, - Courthouse News Service, accessed on April 18, 2025, https://www.courthousenews.com/wp-content/uploads/2024/11/2023-15-8-13-35-15-1-20-cv-00908-RP-2.pdf
34. What the CFTC Says About Binary Options - Silver Law Group, accessed on April 18, 2025, https://www.silverlaw.com/blog/what-the-cftc-says-about-binary-options/
35. Case 1:20-cv-00908-RP Document 128 Filed 03/10/24 Page 1 of 14 - Commodity Futures Trading Commission, accessed on April 18, 2025, https://www.cftc.gov/media/10346/enfjonathancartuorder031024/download
36. Binary Options Experiences - In case of losses, trade immediately. - Law Firm Herfurtner, accessed on April 18, 2025, https://kanzlei-herfurtner.com/binary-options/
37. CFTC Charges 5 Canadians, 1 American, and 4 Companies in $165 Million Global Binary Options Fraud Scheme, accessed on April 18, 2025, https://www.cftc.gov/PressRoom/PressReleases/8231-20
38. Former CEO of Israeli Company Found Guilty of Orchestrating $145 Million Binary Options Fraud Scheme | United States Department of Justice, accessed on April 18, 2025, https://www.justice.gov/archives/opa/pr/former-ceo-israeli-company-found-guilty-orchestrating-145-million-binary-options-fraud-scheme
39. Federal Court Orders International Enterprise to Pay Over $451 Million for Global Binary Options Fraud | CFTC, accessed on April 18, 2025, https://www.cftc.gov/PressRoom/PressReleases/9040-25
40. Europe wide ban on risky binary options - DLA Piper, accessed on April 18, 2025, https://www.dlapiper.com/es-pr/insights/publications/2018/10/finance-and-markets-global-insight-issue-15/europe-wide-ban-on-risky-binary-options
41. ESMA Agrees to Prohibit Binary Options and Restrict CFDs - objectivus, accessed on April 18, 2025, https://objectivus.com/esma-agrees-to-prohibit-binary-options-and-restrict-cfds-to-protect-retail-investors/
42. The end of CFDs and Binary Options? – Why the EU has put a stop & what comes next, accessed on April 18, 2025, https://www.planetcompliance.com/news/the-end-of-cfds-and-binary-options-why-the-eu-has-put-a-stop-what-comes-next/
43. Binary options and CFDs: the AMF adopts national intervention measures - Autorité des marchés financiers, accessed on April 18, 2025, https://www.amf-france.org/en/news-publications/news-releases/amf-news-releases/binary-options-and-cfds-amf-adopts-national-intervention-measures
44. ESMA renews binary options prohibition for a further three months from 2 April 2019, accessed on April 18, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-renews-binary-optio

ns-prohibition-further-three-months-2-april-2019
45. Binary option ban extended, subject to certain exclusions - Taylor Wessing, accessed on April 18, 2025, https://www.taylorwessing.com/en/insights-and-events/insights/2018/09/binary-option-ban-extended-subject-to-certain-exclusions
46. ESMA ceases renewal of product intervention measure relating to binary options, accessed on April 18, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-ceases-renewal-product-intervention-measure-relating-binary-options
47. The Central Bank, Binary Options and CFDs, accessed on April 18, 2025, https://www.mccannfitzgerald.com/knowledge/financial-services-regulation/the-central-bank-binary-options-and-cfds
48. 21-064MR ASIC bans the sale of binary options to retail clients, accessed on April 18, 2025, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2021-releases/21-064mr-asic-bans-the-sale-of-binary-options-to-retail-clients/
49. ASIC extends binary options ban - Money Management, accessed on April 18, 2025, https://www.moneymanagement.com.au/news/policy-regulation/asic-extends-binary-options-ban
50. 22-243MR ASIC's binary options ban extended until 2031, accessed on April 18, 2025, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-243mr-asic-s-binary-options-ban-extended-until-2031/
51. ASIC update: proposal to extend ban on binary options | Addisons | Sydney Law Firm, accessed on April 18, 2025, https://addisons.com/article/asic-update-proposal-to-extend-ban-on-binary-options/
52. ASIC confirms Binary Options ban extension to 2031 - FX News Group, accessed on April 18, 2025, https://fxnewsgroup.com/forex-news/regulatory/asic-confirms-binary-options-ban-extension-to-2031/
53. ASIC Extends Binary Options Ban until October 2031 - Finance Magnates, accessed on April 18, 2025, https://www.financemagnates.com/binary-options/regulation/asic-extends-binary-options-ban-until-october-2031/
54. ASIC's Binary Options Ban Extended - LeapRate, accessed on April 18, 2025, https://www.leaprate.com/binary-options/regulation/asic-binary-options-ban-extended/
55. CFTC pushes for $338.7M fine to be imposed on Yukom, Yossi Herzog, Lee Elbaz, accessed on April 18, 2025, https://fxnewsgroup.com/forex-news/regulatory/cftc-pushes-for-338-7m-fine-to-be-imposed-on-yukom-yossi-herzog-lee-elbaz/
56. Catch of the Week — Yukom Communications and Others Face CFTC Claims of Binary Options Fraud - Constantine Cannon, accessed on April 18, 2025,

https://constantinecannon.com/whistleblower/whistleblower-insider-blog/catch-of-the-week-yukom-communications-and-others-face-cftc-claims-of-binary-options-fraud/

57. UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS COMMODITY FUTURES TRADING COMMISSION, Plaintiff, v. YUKOM C, accessed on April 18, 2025, https://www.cftc.gov/media/11256/enfyakovcohenconsentorder090524/download
58. CFTC Charges Three Individuals with Fraudulently Soliciting U.S. Customers in Binary Options Scheme, accessed on April 18, 2025, https://www.cftc.gov/PressRoom/PressReleases/8025-19
59. Yakov Cohen agrees to pay disgorgement of $7M to settle CFTC charges in binary options lawsuit - FX News Group, accessed on April 18, 2025, https://fxnewsgroup.com/forex-news/regulatory/yakov-cohen-agrees-to-pay-disgorgement-of-7m-to-settle-cftc-charges-in-binary-options-lawsuit/
60. Court Orders $204.6 Million Penalties in CFTC Binary Options Case - Finance Magnates, accessed on April 18, 2025, https://www.financemagnates.com/binary-options/court-orders-2046-million-penalties-in-cftc-binary-options-case/
61. CFTC has hard time finding binary options scammers behind Blue Moon - FX News Group, accessed on April 18, 2025, https://fxnewsgroup.com/forex-news/regulatory/cftc-has-hard-time-finding-binary-options-scammers-behind-blue-moon/
62. CFTC Accepting Whistleblower Award Claims for $204 Million Binary Options Fraud Case, accessed on April 18, 2025, https://whistleblowersblog.org/commodities/cftc-accepting-whistleblower-award-claims-for-204-million-binary-options-fraud-case/
63. Frauds and Scams related to ESMA Logo and ID - European Union, accessed on April 18, 2025, https://www.esma.europa.eu/investor-corner/frauds-and-scams
64. Frauds and Scams visuals, accessed on April 18, 2025, https://www.esma.europa.eu/sites/default/files/2024-03/Frauds_and_Scams.pdf
65. Check before you invest - Moneysmart.gov.au, accessed on April 18, 2025, https://moneysmart.gov.au/check-and-report-scams/check-before-you-invest
66. Report and recover from scams | Cyber.gov.au, accessed on April 18, 2025, https://www.cyber.gov.au/report-and-recover/recover-from/scams
67. Report an investment scam - Moneysmart.gov.au, accessed on April 18, 2025, https://moneysmart.gov.au/check-and-report-scams/report-an-investment-scam
68. Scam alert: Consumers warned about scammers impersonating ASIC requesting funds transfers, accessed on April 18, 2025, https://asic.gov.au/about-asic/news-centre/news-items/scam-alert-consumers-warned-about-scammers-impersonating-asic-requesting-funds-transfers/
69. Report a scam - Scamwatch, accessed on April 18, 2025, https://www.scamwatch.gov.au/report-a-scam
70. Investment scams | Scamwatch, accessed on April 18, 2025, https://www.scamwatch.gov.au/types-of-scams/investment-scams

71. FBI says it's investigating binary options fraud worldwide, invites victims to come forward, accessed on April 18, 2025, https://www.timesofisrael.com/fbi-says-its-investigating-binary-options-fraud-worldwide-invites-victims-to-come-forward/
72. FAQs - | European Securities and Markets Authority, accessed on April 18, 2025, https://www.esma.europa.eu/contact-help/faqs
73. Whistleblowers - | European Securities and Markets Authority, accessed on April 18, 2025, https://www.esma.europa.eu/interact-with-esma/whistleblowers
74. Make a complaint - | European Securities and Markets Authority, accessed on April 18, 2025, https://www.esma.europa.eu/investor-corner/make-complaint
75. Report fraud - European Commission - European Anti-Fraud Office, accessed on April 18, 2025, https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
76. Contact us - ASIC, accessed on April 18, 2025, https://asic.gov.au/about-asic/contact-us/
77. Reporting a tip-off | Australian Financial Security Authority, accessed on April 18, 2025, https://www.afsa.gov.au/contact-us/reporting-tip
78. Investment scams | ASIC, accessed on April 18, 2025, https://asic.gov.au/about-asic/contact-us/reporting-misconduct-to-asic/investment-scams/
79. Reporting misconduct to ASIC, accessed on April 18, 2025, https://asic.gov.au/about-asic/contact-us/reporting-misconduct-to-asic/