Recovering Funds Lost to Binary Options Fraud: A Comprehensive Guide for Victims

Introduction

Falling victim to a binary options scam is a deeply distressing experience, often resulting in significant financial loss and emotional turmoil. These fraudulent schemes are unfortunately prevalent, frequently operating from overseas jurisdictions with sophisticated tactics designed to deceive investors. This report aims to provide a comprehensive guide for individuals who have been defrauded through binary options platforms. It outlines the nature of these scams, details immediate actions to take, explains the crucial process of reporting the fraud, explores potential avenues for fund recovery, and offers guidance on protecting oneself from further harm, including secondary recovery scams. It is imperative, however, to approach the prospect of fund recovery with realistic expectations. Recovering money lost to unregistered, offshore binary options operations is exceptionally challenging and, in many cases, unsuccessful.[1] The primary goal of this report is to empower victims with knowledge and outline every possible step, acknowledging the inherent difficulties involved.

related posts : Best Binary Options Brokers (in 2025)

1. Understanding Binary Options Scams: How They Trap Investors

Comprehending the mechanics and common characteristics of binary options scams is the first step toward navigating the aftermath. These schemes often blend a semblance of legitimate financial activity with outright fraudulent practices.

1.1 What are Binary Options? (Simplified Explanation)

At its core, a binary option is a type of derivative contract where the payout depends entirely on the outcome of a simple yes/no proposition regarding the price movement of an underlying asset (like a stock, commodity, or currency) within a specified, often very short, timeframe.[6] If the investor's prediction is correct, they receive a predetermined fixed payout; if incorrect, they typically lose their entire investment – hence the "all-or-nothing" nature.[9]

Crucially, unlike traditional options, binary options do not grant the holder the right to actually buy or sell the underlying asset.[6] The investor is merely placing a bet on the direction of the price movement. This structure leads many to compare binary options trading to gambling.[7] Furthermore, the payout structure itself can be inherently disadvantageous to the investor. Even with a seemingly fair 50/50 chance of winning, the potential loss (100% of the stake) often significantly outweighs the potential gain

(e.g., a 50-90% return on the stake), resulting in a negative expected return over time for the investor.[8]

1.2 Common Tactics Used by Fraudulent Platforms

Fraudulent binary options platforms employ a consistent set of tactics designed to lure investors and prevent them from withdrawing funds.

- **Offshore & Unregistered Operations:** A defining characteristic is that the vast majority of fraudulent binary options websites operate from overseas locations, often deliberately outside the regulatory reach of the countries where their victims reside.[6] They frequently use fake addresses to suggest a presence in reputable financial centers (like the City of London) while actually being based elsewhere.[7] Critically, these platforms intentionally avoid registering with relevant financial regulatory bodies such as the U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), or the UK's Financial Conduct Authority (FCA).[6] This lack of registration makes regulatory oversight and legal enforcement extremely difficult, if not impossible.
- **Aggressive Marketing & False Promises:** Scammers invest heavily in creating a facade of legitimacy. They utilize social media platforms, professional-looking websites, spam emails, online advertisements, and messaging boards to promote their services.[1] These promotions invariably promise unrealistically high, easy, or even guaranteed returns with little to no risk.[6] To enhance credibility, they often feature fake testimonials, fabricated celebrity endorsements, and enticing images of luxury goods.[1]
- **Targeting Specific Groups:** Evidence suggests scammers may strategically target demographics perceived as more vulnerable or susceptible. This includes retirees, who may have accumulated life savings [10], and younger individuals (under 25s) who are statistically more likely to trust investment offers encountered on social media.[16]
- **High-Pressure Sales & Broker Tactics:** Once initial contact is made, victims are often subjected to high-pressure sales tactics from individuals posing as "brokers" or "account managers".[8] These individuals, frequently operating from scam call centers [10], encourage victims to deposit additional funds, sometimes substantial amounts.[8] Victims may notice a high turnover rate among these representatives.[23] Investigations into large-scale operations have revealed a pervasive culture of intentional deceit, sometimes described by perpetrators themselves as "fun to defraud".[10]
- **Refusal to Process Withdrawals:** A near-universal complaint among victims is the inability to withdraw their deposited funds or supposed profits.[6] Platforms

employ various excuses: ignoring withdrawal requests, phone calls, and emails; arbitrarily freezing accounts; accusing the customer of fraud; or demanding further deposits, fees, or taxes before funds can be released.[6] These are delay tactics often designed to prevent victims from initiating timely disputes with their banks or credit card companies.[23]

- **Software Manipulation:** Numerous reports allege that fraudulent platforms manipulate their trading software to ensure customer losses.[6] A common example cited is the platform extending the expiration time of a winning trade until market conditions change and the trade becomes a loss.[6] This manipulation distorts prices and payouts, making profitable trading virtually impossible.
- **Identity Theft:** Scammers may request excessive personal documentation – such as copies of credit cards, passports, driver's licenses, or utility bills – often under the false pretense of fulfilling regulatory or government requirements.[6] This sensitive information can then be misused for identity theft or sold to other criminals.[6]

1.3 Regulatory Landscape: Bans and Warnings

The pervasive fraud associated with binary options has led regulators worldwide to take significant action.

- In the **United Kingdom**, the FCA banned the sale of binary options to retail consumers effective from April 2, 2019.[7] Any firm currently offering binary options to UK retail clients is likely operating illegally or is a scam.[7]
- In the **European Union**, the European Securities and Markets Authority (ESMA) implemented temporary EU-wide bans starting in July 2018.[26] While ESMA's temporary measures eventually expired, most EU national regulators subsequently implemented permanent national bans or restrictions on binary options for retail clients, effectively making them illegal across the EU.[25]
- In the **United States**, binary options are not entirely banned but are subject to stringent regulation. Only a very limited number of exchanges (currently three: Cantor Exchange LP, Chicago Mercantile Exchange Inc., and NADEX) are designated by the CFTC as contract markets legally permitted to offer binary options to U.S. retail customers.[6] Furthermore, if a binary option meets the definition of a security, its offer and sale must be registered with the SEC, or qualify for an exemption.[6] Most online platforms soliciting US residents do not meet these requirements.

Reflecting the high risk, regulatory agencies maintain warning lists identifying entities operating without authorization or suspected of fraud. These include the CFTC's Registration Deficient (RED) List [6], the FCA's Warning List [7], and the SEC's Public Alert:

Unregistered Soliciting Entities (PAUSE) list.[36]

The near-total ban or severe restriction of binary options for retail investors in major jurisdictions like the UK and EU, coupled with the extremely limited legal avenues in the US, creates a strong presumption of illegitimacy for virtually any unsolicited offer. This regulatory consensus stems directly from the overwhelming evidence of widespread fraud and the inherent risks these products pose to consumers. Any platform offering these products to retail clients without verifiable registration in these regions should be considered highly suspicious.

Furthermore, the remarkable consistency in scam tactics reported by victims and regulators across different countries points towards a globalized fraud methodology. The recurring patterns of withdrawal blocking, software manipulation, aggressive sales, and identity theft attempts suggest these are not isolated incidents but rather standard operating procedures for a widespread network of fraudulent operators.

The combination of sophisticated online marketing, including professional-looking websites and fake reviews [1], with targeted approaches aimed at potentially vulnerable groups [10], demonstrates a calculated and predatory strategy. This underscores the need for extreme skepticism towards any unsolicited binary options investment proposal, regardless of how convincing it may appear.

2. Immediate Actions After Realizing You've Been Scammed

Once the realization dawns that you have been victimized by a binary options scam, swift and decisive action is paramount. Delay can significantly hinder any potential for recovery and may expose you to further risk.

2.1 Step 1: Cease All Contact and Payments

The single most critical immediate step is to **stop sending any more money** to the fraudulent platform or individuals associated with it.[5] Scammers are adept at inventing reasons for additional payments, often framing them as necessary fees, taxes, withdrawal charges, or minimum account balances required to release your initial funds or supposed profits.[37] These are invariably false pretexts designed solely to extract more money. Legitimate financial institutions typically deduct authorized fees directly from an account balance; they do not demand separate, additional payments to access funds.[37]

Simultaneously, **cut off all communication** with the scammers.[5] Do not answer their phone calls, respond to emails, or engage in chats or text messages. Block their

numbers and email addresses if possible. Engaging further only provides them with opportunities to apply more pressure or attempt different deceptive tactics.

2.2 Step 2: Contact Your Financial Institutions (Bank, Credit Card Company)

Immediately notify the fraud departments of all financial institutions through which you transferred funds to the scammers.[2] This includes your bank(s) if you used bank transfers (wires) or debit cards, and your credit card company(ies) if you used credit cards.

It is vital to use the **official contact information** for these institutions, typically found on the back of your card, on official account statements, or on their verified website.[38] Do *not* use phone numbers or links provided by the scammers themselves. In the UK, the dedicated 159 service can securely connect callers to the fraud departments of most major banks.[42]

When contacting them, clearly state:

- That you have been the victim of an online investment scam, specifically involving a fraudulent binary options platform.
- That the transactions related to this platform were unauthorized or based on fraudulent inducement.
- Provide specific transaction details (dates, amounts, recipient information if known).
- Request specific actions:
    - For **credit card** payments: Request they initiate a **chargeback** process due to fraud or services not rendered.
    - For **bank wire transfers**: Request they initiate a **wire recall** or reversal immediately due to fraud.[2]
    - For **debit card** payments: Report the transactions as unauthorized/fraudulent and request a refund investigation.[39]

The effectiveness of these immediate actions hinges critically on timing. Delaying contact with your bank or credit card company drastically reduces the already limited chances of recovering funds. This urgency stems from the mechanics of payment systems. Chargeback procedures have strict time limits, often measured in months or even weeks from the transaction or statement date.[23] Wire transfers are designed for speed and finality; once the funds are moved from the initial receiving bank, recalling them becomes extremely difficult, often impossible.[2] Cryptocurrency transfers are inherently difficult to reverse.[3] Therefore, immediate notification offers the only possibility, however slim, of interrupting these processes before they become fully

irreversible.

2.3 Step 3: Gather All Evidence

Systematically collecting and organizing all evidence related to the scam is crucial.[20] This documentation forms the basis for disputes with financial institutions, reports to regulators and law enforcement, and any potential future legal action.

Compile the following:

- **Communications:** Preserve all emails exchanged with the scammers, ensuring you save the full email headers which contain routing information.[37] Take screenshots of all relevant chat logs (e.g., WhatsApp, Telegram, platform chat), text messages, and social media interactions.[37] Keep detailed notes of any phone conversations, including dates, times, the numbers involved, names used by the representatives, and a summary of what was discussed.[37]
- **Transaction Records:** Gather complete bank statements, credit card statements showing the charges, wire transfer confirmation receipts (including reference numbers, beneficiary bank details, and recipient account information [41]), and detailed records of any cryptocurrency transactions (transaction IDs/hashes, the sending and receiving wallet addresses, exact amounts, cryptocurrency type, dates, and times [3]).
- **Platform Information:** Record the exact website address(es) (URLs) of the fraudulent platform(s).[37] Take comprehensive screenshots of the platform interface, including your account dashboard, purported trade history, promotional materials, deposit/withdrawal pages, and any contact information provided.[37] Note down all names, titles, email addresses, and phone numbers used by the individuals you interacted with.[5]
- **Personal Documentation:** Keep secure copies of any identification documents (passport, driver's license) or other personal information (utility bills, etc.) that you may have unfortunately shared with the scammers.[6] This is important for assessing potential identity theft risks.
- **Timeline of Events:** Construct a detailed, chronological timeline documenting the entire interaction, from the initial contact or advertisement that drew you in, through the deposit process, trading activity (if any), withdrawal attempts, and the realization of the scam.[37]

Organize this information meticulously and keep it in a secure location.[49] This evidence transforms your personal experience into the verifiable data required by banks for disputes [48], by regulators and law enforcement for investigations [5], and by legal counsel should you pursue that route.[20] Without comprehensive documentation,

these crucial subsequent steps are significantly hampered.

3. Reporting the Fraud: Essential Steps and Key Agencies

Reporting the binary options scam to relevant authorities is a critical step, even though it does not guarantee the recovery of lost funds.

3.1 Why Reporting Matters

Taking the time to formally report the fraud serves several vital purposes:

- **Initiates Investigations:** Reporting can trigger investigations by regulatory bodies and law enforcement agencies. While often complex and lengthy, particularly with international elements, these investigations are the only official mechanism that might lead to action against the perpetrators.[49]
- **Aids Prevention and Warnings:** Information from victim reports helps authorities identify fraudulent entities, track scam trends, and issue public warnings.[49] This can lead to entities being added to official warning lists (like the CFTC RED List or FCA Warning List), preventing others from falling victim.[3] In some cases, authorities may be able to shut down scam websites.[3]
- **Creates Official Record:** A formal report creates an official record of the crime. This documentation may be required to support claims with financial institutions or to become eligible for potential future restitution funds if assets are ever recovered through enforcement actions.[20]
- **Contributes to Collective Action:** Each report adds to the body of evidence, helping authorities understand the scale and methods of these operations, potentially leading to more effective enforcement strategies globally.[42]

3.2 Key Reporting Bodies (Jurisdiction-Specific)

It is advisable to report the scam to multiple relevant agencies within your jurisdiction, using the evidence gathered previously. The appropriate agencies depend on your location:

United States:

- **SEC (Securities and Exchange Commission):** File a Tip, Complaint, or Referral (TCR) online via Investor.gov.[15] Relevant if the binary option could be considered a security.
- **CFTC (Commodity Futures Trading Commission):** Submit a tip or complaint online via CFTC.gov.[12] Primary regulator for futures and options; maintains the RED List.[6]
- **FBI (Federal Bureau of Investigation):** File a complaint with the Internet Crime

Complaint Center (IC3) at ic3.gov.[2] Also, consider contacting your local FBI field office, referencing your IC3 complaint number.[5] Handles criminal investigations.
- **FTC (Federal Trade Commission):** Report general consumer fraud and identity theft issues online at ReportFraud.ftc.gov.[2]
- **State Securities Regulator:** Contact the securities regulator in your state. Find contact information through the North American Securities Administrators Association (NASAA) website.[9]
- **FINRA (Financial Industry Regulatory Authority):** File a complaint if you suspect a FINRA-registered broker or firm was involved. Use FINRA BrokerCheck first to verify registration.[6]

United Kingdom:

- **FCA (Financial Conduct Authority):** Report via their online contact form or call 0800 111 6768.[7] Check their Warning List and use the Firm Checker.[7]
- **Action Fraud:** Report online at actionfraud.police.uk or call 0300 123 2040.[38] This is the central reporting point for fraud and cybercrime in England, Wales, and Northern Ireland. You will receive a crime reference number.
- **Police Scotland:** If residing in Scotland, report fraud directly to Police Scotland by calling 101.[38]
- **Citizens Advice:** Provides scam advice and support, and can assist with reporting. Contact their consumer service at 0808 223 1133.[42]

European Union:

- **National Competent Authority (NCA):** Report to the primary financial services regulator in your specific EU member state. ESMA coordinates NCAs but does not handle individual complaints.[35] (Victims should search online for their country's specific financial regulator).
- **National Police:** Report the crime to your national or local police force. They are the primary contact for criminal matters and can liaise with Europol if the case has cross-border implications.[78]
- **Europol:** Europol does **not** accept reports directly from the public.[78] It supports investigations initiated by national law enforcement agencies.[79] Reporting to your national police is the correct procedure.

International / Other:

- **IOSCO (International Organization of Securities Commissions):** While not a direct enforcement body for individuals, victims can check for alerts related to the entity on the IOSCO I-SCAN portal and potentially report suspicious entities, contributing to global awareness.[83]

- **Local Law Enforcement:** Regardless of where the scam originates, filing a report with your local police department is generally advisable and often a necessary first step.[3]

The complexity of the reporting landscape, with different agencies overseeing regulatory compliance, criminal activity, and consumer protection, underscores the importance of reporting to *multiple* relevant bodies. This multi-pronged approach ensures the incident is reviewed from various perspectives (financial regulation, criminal law, consumer rights), maximizing the chances that some form of official action might be taken, even if direct fund recovery remains elusive.

For scams involving international elements, the victim's primary point of contact should always be their *national* authorities (regulators and law enforcement). While international organizations like IOSCO and Europol play vital coordinating roles [78], they operate through their member national agencies. Directing victims to their home country's authorities first is the procedurally correct and most practical path; these national bodies can then engage international cooperation channels as needed.

3.3 Table 1: Key Reporting Agencies and Contact Information

To assist victims in navigating this process, the following table summarizes key reporting bodies:

Jurisdiction	Agency	Primary Role	Reporting Method (Link/Phone Preferred)	Supporting Snippets
United States	SEC	Securities Regulation	Online TCR Portal (Investor.gov)	21
	CFTC	Commodities/Futures/Options Regulation	Online Tip/Complaint Form (CFTC.gov)	12
	FBI	Criminal Investigation	IC3.gov (Online Complaint) / Local Field Office	41

	FTC	Consumer Fraud / ID Theft	ReportFraud.ftc.gov (Online)	[49]
	State Securities Regulator	State-Level Securities Regulation	Via NASAA website (nasaa.org)	[49]
United Kingdom	FCA	Financial Regulation	Online Contact Form / 0800 111 6768	[7]
	Action Fraud	National Fraud Reporting (Eng/Wal/NI)	actionfraud.police.uk / 0300 123 2040	[42]
	Police Scotland	Law Enforcement (Scotland)	Call 101	[38]
	Citizens Advice	Victim Support & Guidance	0808 223 1133	[42]
European Union	National Competent Authority (NCA)	National Financial Regulation	Varies by Country (Search Required)	[35]
	National Police	Criminal Investigation	Varies by Country (See [78])	[78]
International	IOSCO	International Regulatory Cooperation	I-SCAN Portal (iosco.org/i-scan/)	[83]
	Local Police	Initial Crime Report	Local Police Department Contact	[3]

Note: This table provides primary contacts. Additional agencies may be relevant depending on specific circumstances.

4. Exploring Recovery Avenues: Realities and Procedures

While challenging, exploring all potential avenues for fund recovery is essential. The

viability of each option depends heavily on the payment method used, the speed of action, and the nature/location of the fraudulent entity.

4.1 Credit/Debit Card Chargebacks

If funds were deposited using a credit or debit card, initiating a chargeback is often the most direct route to potential recovery.

- **Process:** The cardholder must contact their issuing bank (the bank that issued the card) to dispute the transaction(s).[51] The bank reviews the claim based on the rules set by the card network (e.g., Visa, Mastercard).[87] The bank may issue a provisional credit to the cardholder while investigating.[48] The merchant (the scam platform, via their acquiring bank) is notified and has the right to contest the chargeback by providing evidence.[48] The process can involve multiple cycles (first chargeback, second chargeback/pre-arbitration) before the issuing bank makes a final decision.[48] Arbitration by the card network is a final, but costly, step.[48]
- **Time Limits:** Chargeback rights are time-sensitive. Deadlines vary by card network and the specific reason code for the dispute, but typically range from 45 to 180 days from the transaction date or statement date.[48] In the US, the Fair Credit Billing Act (FCBA) offers protections, but requires written dispute within 60 days of the first bill containing the error.[23] Acting promptly is crucial.
- **Evidence:** Success often depends on providing compelling evidence to the issuing bank demonstrating the fraudulent nature of the transaction or that services paid for were not rendered as promised.[48] The evidence gathered in Section 2.3 is vital here.
- **Reason Codes:** Chargebacks are categorized by reason codes (e.g., unauthorized transaction, merchandise/services not received).[88] The applicability of a chargeback depends on whether the situation fits an allowable reason code under the network rules.
- **Likelihood:** While possible, chargeback success is not guaranteed.[51] Merchants, facing lost revenue and chargeback fees (estimated at $15-$70 per dispute for Mastercard [51]), may vigorously dispute the claim. Some law firms have reported success using chargebacks for financial scam victims.[90]

4.2 Bank Wire Transfer Recalls

Recovering funds sent via bank wire transfer is significantly more difficult than chargebacks.

- **Process:** The sender must immediately contact their bank's fraud department upon discovering the fraud.[2] Request the bank initiate a wire recall (often via the SWIFT network for international transfers) or reversal, explicitly stating it was due

to fraud.[2]

- **Time Sensitivity:** This is extremely time-critical. A recall is generally only possible if the funds have not yet been credited to the recipient's account or moved onward by the recipient.[2] Fraudsters typically move funds very quickly once received.
- **Difficulty:** Success requires the cooperation of the receiving bank and potentially intermediary banks.[2] If the receiving bank refuses or the funds are already gone, the recall will fail.
- **Likelihood:** The probability of successfully recalling a fraudulent wire transfer is very low, often described as "almost impossible" [2] or having low chances.[40] Rapid reporting (within hours or a few days) offers the only slim possibility.[41]

4.3 Cryptocurrency Payments: The Recovery Challenge

Recovering cryptocurrency sent to scammers presents unique and formidable challenges.

- **Irreversibility:** Cryptocurrency transactions are, by design, generally irreversible.[3] Once a transaction is confirmed on the blockchain, it cannot be unilaterally cancelled or reversed by the sender or their bank/exchange. Recovery typically requires the recipient to voluntarily send the funds back, which scammers will not do.
- **Reporting Steps (Low Success Chance):**
  - **Notify Exchange/Platform:** If a centralized exchange was used for the transfer, report the fraud to them immediately.[4] Provide all transaction details. While not obligated, a cooperative exchange *might* freeze the scammer's account *if* the funds are still there and *if* they respond to law enforcement requests. However, many scam platforms are unregulated or complicit.
  - **Report to Law Enforcement:** File reports with the FBI (IC3), local police, and relevant financial regulators (SEC, CFTC), providing all transaction hashes, wallet addresses involved, dates, times, and amounts.[3]
  - **Blockchain Analysis:** Specialized firms or law enforcement can use blockchain analysis tools to trace the movement of stolen funds across public ledgers.[3] Tracing can identify wallets holding the funds but does not automatically lead to recovery. It primarily aids investigation and potential future asset seizure if perpetrators are identified and located. Victims should be extremely wary of private tracing companies promising recovery (see Section 5).
- **Likelihood:** The chance of recovering cryptocurrency lost to scams is exceptionally low.[4] Scammers often use techniques like tumblers/mixers or rapidly

move funds through multiple wallets across different blockchains and jurisdictions to obscure the trail and make seizure nearly impossible.

4.4 Regulatory Restitution and Legal Actions

Beyond direct payment disputes, other avenues involve intervention by authorities or the legal system.

- **Regulatory Restitution:** Financial regulators like the SEC and CFTC sometimes recover funds through successful enforcement actions against fraudulent entities.[19] These recovered assets may be distributed to harmed investors through mechanisms like SEC Fair Funds or the CFTC Reparations Program.[19]
    - *Limitations:* This is entirely dependent on the regulator successfully prosecuting the case and seizing sufficient assets from the perpetrators, which may be difficult, especially if they are offshore.[1] Recovered amounts often represent only a small fraction of total investor losses. The process can take many years, and eligible victims are typically notified automatically by the agency or a court-appointed administrator.[52]
- **Arbitration/Mediation:** This is a dispute resolution process primarily available for conflicts with *registered* brokerage firms or brokers, often facilitated by organizations like FINRA in the US.[19] It is generally faster and less formal than court litigation.[52] However, it is unlikely to be applicable to the typical unregistered, offshore binary options platform. Filing fees apply (though waivers may be available), and there are time limits (e.g., six years for FINRA claims).[52]
- **Private Lawsuits/Class Actions:** Victims retain the right to pursue private civil lawsuits against the individuals and entities responsible for the fraud.[19] When numerous victims exist, these may be consolidated into class action lawsuits.[19]
    - *Challenges:* Significant hurdles exist, including identifying and locating defendants, especially if they operate offshore using aliases.[25] Enforcing judgments across international borders is complex and costly. Proving fraud legally, distinct from mere investment losses due to market risk, requires substantial evidence.[20] Legal fees can be prohibitive, although some specialized law firms may take such cases on a contingency basis.[92] Despite the difficulties, successful class actions recovering substantial sums have occurred in some large-scale financial fraud cases.[25] Notably, traders of options related to a stock can potentially be included in securities fraud class actions.[93]
- **Insolvency/Bankruptcy Proceedings:** If the fraudulent entity formally declares bankruptcy or becomes insolvent, victims may be able to file a claim as creditors in the bankruptcy proceedings.[45]

- *Limitations:* Recovery depends entirely on the company having identifiable assets remaining after secured creditors are paid. Unsecured investors are typically low on the priority list and often receive little to nothing.[94] The process is managed through the courts and can be lengthy.[52]

The initial payment method used fundamentally dictates the immediate recovery path and its potential success. Card payments offer the structured, albeit time-limited and not guaranteed, chargeback mechanism. Wire transfers and cryptocurrency payments, due to their speed and finality characteristics, offer far lower prospects for direct reversal.

Beyond these initial disputes, any hope for recovery shifts heavily towards external factors: the success of regulatory or law enforcement actions in locating perpetrators and seizing assets (a difficult task with international criminals), or navigating complex, expensive, and uncertain legal battles. These longer-term avenues require significant patience and offer no guarantees, often yielding minimal results for victims of offshore, unregistered schemes.

4.5 Table 2: Comparison of Fund Recovery Methods

Method	Process Overview	Typical Timeframe	Likelihood of Success	Key Considerations & Challenges	Supporting Snippets
Credit/Debit Card Chargeback	Contact issuing bank; bank investigates based on network rules; merchant can dispute.	Initiate within 45-180 days (varies); resolution weeks to months.	Moderate (if timely & evidence strong).	Strict deadlines; requires compelling evidence; merchant may fight; depends on reason code.	23
Bank Wire Transfer Recall	Contact sending bank immediately; request recall (e.g., SWIFT); bank	Must act within hours/days; success depends on funds not being	Very Low.	Extremely time-sensitive; requires receiving bank cooperation; funds often	2

	attempts to retrieve funds.	moved.		moved quickly.	
Cryptocurrency Recovery	Report to exchange (if used) & law enforcement; blockchain tracing possible.	Immediate reporting needed; recovery highly unlikely.	Extremely Low.	Transactions largely irreversible; requires recipient cooperation (won't happen); tracing ≠ recovery; beware recovery scams.	[3]
Regulatory Restitution	Funds recovered via successful gov't enforcement action distributed to victims.	Years.	Low to Moderate (if action successful & assets seized).	Dependent on successful prosecution & asset seizure; often partial recovery; automatic notification if eligible.	[1]
Legal Action (Lawsuit/Class Action)	File civil suit against perpetrators; class action joins multiple victims.	Years.	Low (esp. vs offshore entities).	High cost; difficulty locating/serving offshore defendants; complex international enforcement; proving fraud.	[19]
Bankruptcy Claim	File claim as creditor if fraudulent company	Years.	Very Low (for unsecured investors).	Recovery depends on remaining assets after	[45]

	enters bankruptcy.			secured creditors; often minimal/no payout.	

5. Beware: The Danger of Recovery Scams

Tragically, individuals who have already lost money to scams are frequently targeted again by secondary scams known as "recovery scams".[5] These predators exploit the victim's desperation to recoup their losses.

5.1 How Recovery Scams Target Victims

Scammers obtain victims' contact details through various means, including purchasing or trading "sucker lists" which contain information about people previously defrauded [70], or by scouring public court filings related to fraud cases.[57] In some instances, the recovery scammers may be the same individuals who perpetrated the original fraud, or their associates.[60]

The typical approach involves unsolicited contact – via phone call, email, text message, social media, or even postal mail – offering assistance in recovering the funds lost in the initial scam.[57] These recovery scammers often possess specific details about the original fraud to make their pitch seem more credible.[61]

5.2 Red Flags of Fraudulent Recovery Services

Recognizing the warning signs of a recovery scam is crucial to avoid further financial loss. Be extremely wary if any of the following occur:

- **Upfront Fees:** This is the most significant red flag. Scammers demand payment *before* any funds are supposedly recovered.[9] They may call this fee a retainer, processing fee, tax, insurance bond, donation, or something similar. Legitimate government recovery efforts do not require upfront payments from victims.
- **Guarantees:** Promises or guarantees of recovering your lost funds, or claims of exceptionally high success rates, are hallmarks of a scam.[59] Fund recovery from sophisticated fraud is inherently uncertain and never guaranteed.
- **Government Impersonation:** Scammers frequently claim to be affiliated with official government agencies (like the SEC, FBI, FTC, CFTC, Treasury Department, courts) or legitimate law firms or consumer groups to gain trust.[3] Always verify such claims independently. Remember official US government websites end in .gov or .fed.us, and officials typically communicate via official mail or these domains, not personal email accounts.[61]

- **Requests for Sensitive Information:** Be suspicious if asked for highly sensitive personal or financial information, such as bank account numbers, credit card details, Social Security numbers, or cryptocurrency wallet private keys/passphrases, often under the guise of needing it to deposit the recovered funds.[59]
- **Insistence on Specific Payment Methods:** Scammers often demand that their upfront fees be paid via methods that are difficult to trace or reverse, such as wire transfers, cryptocurrency (Bitcoin, Tether, etc.), or gift cards.[46] Legitimate entities rarely restrict payments to these methods.
- **Unprofessionalism:** Look for signs like poorly designed websites, lack of a verifiable physical address (or an address that appears fake upon checking via online maps [15]), absence of a legitimate customer service phone number, communication primarily via messaging apps (WhatsApp, Telegram [5]), use of free web-based email addresses (@gmail.com, @yahoo.com [59]), and poor grammar or spelling in communications.[15]
- **Fake Credentials and Reviews:** Scammers create fake testimonials, publish misleading press releases picked up by automated news feeds, claim non-existent awards, or assert they have special "insider access" or proprietary technology to recover funds.[59]
- **Discouraging Official Reporting:** Some recovery scammers may advise victims *not* to report the original fraud to the police or regulators, which is counter to legitimate advice.[72]

5.3 Verifying Legitimate Assistance vs. Scams

Distinguishing genuine help from a recovery scam requires vigilance:

- **Government Agencies Don't Charge Fees:** Remember that legitimate government agencies involved in investigating financial fraud (FBI, SEC, CFTC, FTC, etc.) and court-appointed administrators handling restitution funds will **never** ask victims to pay a fee to assist in an investigation or to receive their share of any recovered money.[23] This "no upfront fee" principle is the most reliable indicator of legitimacy for government-related recovery efforts. Any request for payment from someone claiming government affiliation is a scam.
- **Caution with Third-Party Companies:** Exercise extreme caution before engaging any private company offering asset recovery services.[57] Thoroughly research the company online, searching for its name along with terms like "scam," "complaint," or "review".[70] If they claim legal or financial expertise, verify their credentials and registration with relevant professional bodies. Ask precisely what services they will perform for the fee and assess if these are actions you could

take yourself for free (like filing regulatory complaints).[57]

- **Crypto Recovery Specifics:** Be particularly skeptical of services claiming they can recover stolen cryptocurrency through hacking, special access to exchanges, or reversing blockchain transactions.[3] These claims are almost always false. Legitimate crypto recovery typically involves data recovery specialists helping retrieve lost private keys from damaged devices, not undoing fraudulent transfers.[59]
- **Independent Verification:** If contacted unexpectedly by someone claiming to represent a government agency, court, or legitimate company, **always verify their identity independently**. Do not use phone numbers, email addresses, or website links provided by the person who contacted you. Instead, find the official contact information for the organization through a separate, trusted source (like an official government website or directory) and initiate contact yourself to confirm the legitimacy of the outreach.[61]

The existence of a thriving secondary scam industry targeting fraud victims underscores the critical need to maintain skepticism throughout the recovery process. Scammers adeptly exploit the emotional vulnerability and desperation of those seeking to reclaim lost funds. Applying the same critical evaluation to recovery offers as should have been applied to the initial investment is essential protection against further victimization.

6. Protecting Yourself from Further Harm

After falling victim to a scam, it's crucial to take steps to protect your remaining assets and personal information from potential misuse or future attacks.

6.1 Monitoring Accounts and Credit Reports

Since personal and potentially financial information may have been compromised during the scam, ongoing vigilance is necessary.

- **Monitor Financial Accounts:** Regularly review all bank account and credit card statements for any transactions you do not recognize.[23] Report any suspicious activity immediately to the respective institution.
- **Check Credit Reports:** Obtain and review your credit reports from the major credit bureaus (Experian, Equifax, TransUnion). Look for any accounts or inquiries you did not authorize. Victims of financial fraud should consider placing protective measures on their credit files.[49]
- **Fraud Alerts:** Place an initial fraud alert on your credit reports. This alerts potential creditors to verify your identity before issuing new credit in your name.[39]

- **Credit Freezes:** For stronger protection, consider a credit freeze (or security freeze), which restricts access to your credit report, making it much harder for identity thieves to open new accounts.[39]

6.2 Securing Online Accounts

Strengthening the security of your online presence is vital, especially for accounts linked to finances or those potentially accessed by scammers.

- **Change Passwords:** Immediately change the passwords for any online accounts associated with the scam, including email accounts used for communication, online banking portals, and any cryptocurrency exchange accounts.[42] Use strong, unique passwords for each account.
- **Enable Two-Factor Authentication (2FA):** Activate 2FA (also known as multi-factor authentication or MFA) wherever possible, particularly for financial accounts, email, and crypto exchanges.[50] Prioritize using authenticator apps (like Google Authenticator or Authy) over SMS-based 2FA, as SMS can be vulnerable to hijacking.[59]
- **Antivirus/Malware Scans:** Run comprehensive scans using reputable antivirus and anti-malware software on any computers or devices used to interact with the fraudulent platform or communicate with the scammers.[42]

6.3 Recognizing Future Scam Attempts

Victims of fraud are often targeted again.[7] Maintaining a heightened sense of awareness and skepticism is crucial.

- **Be Wary of Unsolicited Contact:** Treat any unsolicited investment offers, requests for personal information, or demands for payment with extreme caution, whether received via phone, email, text, or social media.[17]
- **Resist Pressure:** Be alert to high-pressure sales tactics or claims of urgency designed to rush you into a decision.[18] Legitimate opportunities allow time for due diligence.
- **Verify Independently:** If contacted unexpectedly by someone claiming to represent a known business or government agency, always verify the contact independently using official channels before sharing information or taking action.[61]
- **Internalize Due Diligence:** The most effective defense against future scams is proactive due diligence. Before engaging with any investment platform or financial professional, verify their registration and background status with the appropriate regulatory bodies (e.g., SEC, CFTC, FCA, FINRA BrokerCheck, NFA BASIC).[6] The consistent advice from regulators underscores that checking

registration *before* investing is the simplest way to filter out a vast number of fraudulent operators. Applying this hard-learned lesson is key to protecting oneself moving forward.

7. Conclusion: Navigating the Path Forward and Resources

Recovering from a binary options scam is an arduous process, fraught with challenges and uncertainty. While the prospects of fully recovering lost funds are often slim, particularly when dealing with unregistered offshore entities utilizing wire transfers or cryptocurrency, taking systematic action is still essential.

7.1 Summary of Key Actions and Realistic Expectations

The critical immediate steps involve ceasing all contact and payments to the scammers, promptly notifying all relevant financial institutions to attempt chargebacks or recalls, and meticulously gathering all evidence pertaining to the fraud. Subsequently, reporting the incident comprehensively to multiple appropriate authorities – including financial regulators (SEC, CFTC, FCA), law enforcement (FBI/IC3, Action Fraud, national/local police), and consumer protection agencies (FTC) – is vital for initiating investigations, warning others, and creating an official record.

Exploring recovery avenues requires understanding the limitations of each method. Chargebacks offer the most structured process but are time-limited and not guaranteed. Wire recalls and cryptocurrency recovery are exceedingly difficult due to the speed and nature of these transfers. Longer-term possibilities like regulatory restitution or legal action depend heavily on external factors beyond the victim's control and often yield partial or no recovery after lengthy periods. It is crucial to maintain realistic expectations: full recovery is rare. Equally important is vigilance against secondary recovery scams, recognizing that legitimate government assistance never requires upfront fees.

7.2 List of Reputable Resources for Victims

Victims seeking information and channels for reporting can consult the following official resources:

- **United States:**
  - SEC Office of Investor Education and Advocacy (OIEA): Investor.gov [8]
  - CFTC Consumer Protection: cftc.gov/LearnAndProtect [12]
  - FBI Internet Crime Complaint Center: ic3.gov [5]
  - Federal Trade Commission: ReportFraud.ftc.gov [70]
  - FINRA Investor Information: finra.org/investors [52]

    - North American Securities Administrators Association (for State Regulators): nasaa.org [49]
- **United Kingdom:**
    - Financial Conduct Authority (FCA) ScamSmart: fca.org.uk/scamsmart [7]
    - Action Fraud: actionfraud.police.uk [74]
    - Citizens Advice: citizensadvice.org.uk/scamsadvice [42]
- **International:**
    - International Organization of Securities Commissions (IOSCO): I-SCAN Portal (iosco.org/i-scan/) [83]

For emotional support, resources like the VictimConnect Resource Center (US) [49] or Citizens Advice (UK) [77] may offer guidance or referrals.

7.3 Final Encouragement

While the path after being scammed is undeniably difficult, taking informed action provides a measure of control in a challenging situation. By understanding the scam, acting swiftly, reporting thoroughly, exploring avenues realistically, guarding against further deception, and utilizing available resources, victims can navigate the aftermath with greater clarity and work towards protecting themselves in the future.

Works cited

1. Binary Options fraud leads to $13.8M fine for Peter Szatmari - FX News Group, accessed April 24, 2025, https://fxnewsgroup.com/forex-news/regulatory/binary-options-fraud-leads-to-13-8m-fine-for-peter-szatmari/
2. Wire transfer fraud: definition, strategies and recovery - Trustpair, accessed April 24, 2025, https://trustpair.com/blog/wire-transfer-fraud-prevention-best-practices-and-recovery/
3. Beware Cryptocurrency Scams - Mass.gov, accessed April 24, 2025, https://www.mass.gov/info-details/beware-cryptocurrency-scams
4. How to recover lost cryptocurrency—and how to keep it safe - Britannica, accessed April 24, 2025, https://www.britannica.com/money/cryptocurrency-recovery-safety
5. Cryptocurrency Investment Fraud - FBI, accessed April 24, 2025, https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud
6. Binary Options Fraud - FBI, accessed April 24, 2025, https://www.fbi.gov/news/stories/binary-options-fraud
7. Binary options scams | FCA, accessed April 24, 2025, https://www.fca.org.uk/consumers/binary-options-scams

8. Binary Options Fraud | Investor.gov, accessed April 24, 2025, https://www.investor.gov/protect-your-investments/fraud/types-fraud/binary-options-fraud
9. Beware of Online Binary Options Schemes - Missouri Secretary of State, accessed April 24, 2025, https://www.sos.mo.gov/bewareofonlinebinaryoptionsschemes
10. Fraudulent binary options scheme participants ordered to pay CFTC $451m, accessed April 24, 2025, https://www.grip.globalrelay.com/defendants-who-operated-fraudulent-binary-options-scheme-ordered-to-pay-cftc-451m/
11. Binary Options Experiences - In case of losses, trade immediately. - Law Firm Herfurtner, accessed April 24, 2025, https://kanzlei-herfurtner.com/binary-options/
12. Binary Options Fraud | CFTC, accessed April 24, 2025, https://www.cftc.gov/BinaryOptionsFraud/index.htm
13. FCA issues list of unauthorised binary options providers, accessed April 24, 2025, https://www.fca.org.uk/news/press-releases/fca-issues-list-unauthorised-binary-options-providers
14. CFTC/SEC Investor Alert: Binary Options and Fraud, accessed April 24, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/fraudadv_binaryoptions.html
15. 10 SIGNS OF A SCAM CRYPTO OR FOREX TRADING WEBSITE, accessed April 24, 2025, https://www.cftc.gov/sites/default/files/2023-04/SpotFraudSites.pdf
16. FCA warns of increased risk of online investment fraud, as investors lose £87k a day to binary options scams, accessed April 24, 2025, https://www.fca.org.uk/news/press-releases/fca-warns-increased-risk-online-investment-fraud-investors-scamsmart
17. Investment Scams | Consumer Advice - Federal Trade Commission, accessed April 24, 2025, https://consumer.ftc.gov/features/pass-it-on/investment-scams
18. Investment Scams | Consumer Advice - Federal Trade Commission, accessed April 24, 2025, https://consumer.ftc.gov/articles/investment-scams
19. Investment Fraud: 22 Scams To Know of (and Avoid) Right Now - Aura, accessed April 24, 2025, https://www.aura.com/learn/investment-fraud
20. Have you been subjected to binary options fraud? - New York City Securities Litigation Lawyer, accessed April 24, 2025, https://www.denninlaw.com/2021/09/have-you-been-subjected-to-binary-options-fraud/
21. What You Need to Know about Investment Scams - TN.gov, accessed April 24, 2025, https://www.tn.gov/attorneygeneral/working-for-tennessee/consumer/resources/materials/investment-scams.html
22. What To Know About Cryptocurrency and Scams - Federal Trade Commission, accessed April 24, 2025, https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams
23. Investor Alert: Binary Options Websites may be Used for Fraudulent Schemes,

accessed April 24, 2025, https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-4
24. BeeOptions operators hit with $204M US court order in Binary Options fraud, accessed April 24, 2025, https://fxnewsgroup.com/forex-news/regulatory/beeoptions-operators-hit-with-204m-us-court-order-in-binary-options-fraud/
25. Giambrone continues the Fight for compensation for Victims of Banc de Binary, accessed April 24, 2025, https://www.giambronelaw.com/site/news-articles-press/library/articles/giambrone-fights-for-compensation-for-victims-banc-de-binary
26. The end of CFDs and Binary Options? – Why the EU has put a stop & what comes next, accessed April 24, 2025, https://www.planetcompliance.com/news/the-end-of-cfds-and-binary-options-why-the-eu-has-put-a-stop-what-comes-next/
27. Central Bank of Ireland Binary Options Intervention Measure pursuant to Article 42 of Regulation (EU) No 600/2014 of the European Parliament, accessed April 24, 2025, https://www.centralbank.ie/docs/default-source/Regulation/industry-market-sectors/investment-firms/mifid-firms/regulatory-requirements-and-guidance/central-bank-binary-options-intervention-measure.pdf
28. ESMA renews binary options prohibition for a further three months from 2 January 2019, accessed April 24, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-renews-binary-options-prohibition-further-three-months-2-january-2019
29. ESMA renews binary options prohibition for a further three months from 2 April 2019, accessed April 24, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-renews-binary-options-prohibition-further-three-months-2-april-2019
30. Notice of ESMA's Product Intervention Renewal Decision in relation to binary options, accessed April 24, 2025, https://www.esma.europa.eu/press-news/esma-news/notice-esma%E2%80%99s-product-intervention-renewal-decision-in-relation-binary-option-1
31. EU Product Intervention Measures for Binary Options Extended - A&O Shearman | FinReg, accessed April 24, 2025, https://finreg.aoshearman.com/eu-product-intervention-measures-for-binary-optio
32. ESMA adopts final product intervention measures on CFDs and binary options, accessed April 24, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-adopts-final-product-intervention-measures-cfds-and-binary-options
33. ESMA agrees to prohibit binary options and restrict CFDs to protect retail investors, accessed April 24, 2025, https://www.centralbank.ie/regulation/markets-update/esma-guidelines-and-recommendations/markets-update-issue-6-2018/european-securities-and-markets-a

uthority-(esma)/esma-agrees-to-prohibit-binary-options-and-restrict-cfds-to-protect-retail-investors
34. Europe wide ban on risky binary options - DLA Piper, accessed April 24, 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
35. ESMA ceases renewal of product intervention measure relating to binary options, accessed April 24, 2025, https://www.esma.europa.eu/press-news/esma-news/esma-ceases-renewal-product-intervention-measure-relating-binary-options
36. Public Alert: Unregistered Soliciting Entities (PAUSE) - SEC.gov, accessed April 24, 2025, https://www.sec.gov/enforcement-litigation/public-alerts-unregistered-soliciting-entities
37. 6 Steps to Take after Discovering Fraud | CFTC, accessed April 24, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/6Steps.html
38. Report a scam | FCA, accessed April 24, 2025, https://www.fca.org.uk/consumers/report-scam
39. Do banks refund scammed money? How to recover your money - ExpressVPN, accessed April 24, 2025, https://www.expressvpn.com/blog/do-banks-refund-scammed-money/
40. What to do if your wire transfer is lost - Wise, accessed April 24, 2025, https://wise.com/us/blog/lost-wire-transfer
41. How to Make Sure You Are Secure After Wire Fraud | CertifID, accessed April 24, 2025, https://www.certifid.com/article/how-to-recover-from-wire-fraud
42. How to protect yourself from financial scams - Citizens Advice Wiltshire, accessed April 24, 2025, https://www.citizensadvicewiltshire.org.uk/news1/103-how-to-protect-yourself-from-financial-scams
43. How to protect yourself from financial scams - Citizens Advice Wiltshire, accessed April 24, 2025, https://citizensadvicewiltshire.org.uk/component/content/article/103-how-to-protect-yourself-from-financial-scams?catid=19:front-page-news&Itemid=537
44. Being #ScamAware - Citizens Advice County Durham, accessed April 24, 2025, https://www.citizensadvicecd.org.uk/scamaware/
45. Investment Fraud: What You Need To Know And How To Protect Your Investments, accessed April 24, 2025, https://www.bankruptcyattorneys.org/investment-fraud-what-you-need-to-know-and-how-to-protect-your-investments/
46. What to Do if You've Lost Money in a Scam | Georgia Attorney General's Consumer Protection Division, accessed April 24, 2025, https://consumer.georgia.gov/scams-what-do-if-youve-lost-money-scam
47. Check if you can get your money back after a scam - Citizens Advice, accessed April 24, 2025, https://www.citizensadvice.org.uk/consumer/scams/check-if-you-can-get-your-money-back-after-a-scam/

48. The Chargeback Process for Merchants: Fighting & Winning Disputes - Signifyd, accessed April 24, 2025, https://www.signifyd.com/resources/fraud-101/chargeback-dispute-process-for-merchants/
49. Recovering from Investment Fraud: Start with These 6 Steps | FINRA.org, accessed April 24, 2025, https://www.finra.org/investors/insights/recovering-from-investment-fraud
50. How to Recover from a Crypto Scam: Steps to Take Immediately - OSL, accessed April 24, 2025, https://osl.com/academy/article/how-to-recover-from-a-crypto-scam-steps-to-take-immediately
51. What is a chargeback? - Mastercard, accessed April 24, 2025, https://b2b.mastercard.com/news-and-insights/blog/what-is-a-chargeback/
52. Legitimate Avenues for Recovery of Investment Losses | FINRA.org, accessed April 24, 2025, https://www.finra.org/investors/need-help/legitimate-avenues-recovery-investment-losses
53. Resources for Victims of Securities Law Violations | Investor.gov, accessed April 24, 2025, https://www.investor.gov/protect-your-investments/fraud/resources-victims-securities-law-violations
54. Reporting fraud - Stop! Think Fraud, accessed April 24, 2025, https://stopthinkfraud.campaign.gov.uk/reporting-fraud/
55. NASAA Informed Investor Advisory: Binary Options -, accessed April 24, 2025, https://www.nasaa.org/43192/informed-investor-advisory-binary-options/
56. Criminal Division | Report Fraud - Department of Justice, accessed April 24, 2025, https://www.justice.gov/criminal/criminal-fraud/report-fraud
57. Investor Alert: What You Should Know About Asset Recovery Companies, accessed April 24, 2025, https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-33
58. Recover from Scams | Office of the Vermont Attorney General, accessed April 24, 2025, https://ago.vermont.gov/cap/recover-scams
59. Are Crypto Recovery Services a Scam? How To Be Sure - Aura, accessed April 24, 2025, https://www.aura.com/learn/crypto-recovery-service-scams
60. Relationship Cons, Recovery Scams, & Money Laundering | CFTC, accessed April 24, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/Fraudin3Acts.html
61. Don't be Re-Victimized by Recovery Frauds | CFTC, accessed April 24, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/RecoveryFrauds.html
62. Steps to File A Cybercrime Report with the FBI's IC3 - Digital Forensics Corp, accessed April 24, 2025, https://www.digitalforensics.com/blog/extortion/report-cybercrime-to-the-fbi/
63. Cybercrime | Federal Bureau of Investigation - FBI, accessed April 24, 2025,

https://www.fbi.gov/investigate/cyber
64. White-Collar Crime - FBI, accessed April 24, 2025, https://www.fbi.gov/investigate/white-collar-crime
65. Common Frauds and Scams - FBI, accessed April 24, 2025, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams
66. Scams and Safety - FBI, accessed April 24, 2025, https://www.fbi.gov/how-we-can-help-you/scams-and-safety
67. — Seeking Victims in Banc de Binary Investor Fraud Scheme - FBI.gov, accessed April 24, 2025, https://forms.fbi.gov/seeking-victims-in-banc-de-binary-investor-fraud-scheme
68. FBI San Diego Seizes Cryptocurrency Recovery Websites, accessed April 24, 2025, https://www.fbi.gov/contact-us/field-offices/sandiego/news/fbi-san-diego-seizes-cryptocurrency-recovery-websites
69. Business and Investment Fraud - FBI, accessed April 24, 2025, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-and-investment-fraud
70. Refund and Recovery Scams | Consumer Advice - Federal Trade Commission, accessed April 24, 2025, https://consumer.ftc.gov/articles/refund-and-recovery-scams
71. New FTC Data Spotlight highlights text scams that may target your business, accessed April 24, 2025, https://www.ftc.gov/node/88079
72. It Can Be Hard to Recover from 'Recovery' Scams | FINRA.org, accessed April 24, 2025, https://www.finra.org/investors/insights/recovery-scams
73. Options | FINRA.org, accessed April 24, 2025, https://www.finra.org/investors/investing/investment-products/options
74. Cyber crime - Fraud - Police.uk, accessed April 24, 2025, https://www.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/
75. Fraud Reporting: 5 Simple Steps | Fraud Prevention - Skillcast, accessed April 24, 2025, https://www.skillcast.com/blog/fraud-reporting-simple-steps
76. How To Report Fraud - Action Fraud Claims Advice, accessed April 24, 2025, https://www.actionfraud.org.uk/report_fraud/
77. Advice on scams, accessed April 24, 2025, https://www.citizensadvice.org.uk/about-us/information/advice-on-scams/
78. Report a Crime | Europol - European Union, accessed April 24, 2025, https://www.europol.europa.eu/report-a-crime
79. Europol Published Practical Guide for Cooperation Between Financial Institutions and Investigative Authorities | Skadden, Arps, Slate, Meagher & Flom LLP, accessed April 24, 2025, https://www.skadden.com/insights/publications/2025/02/europol-published
80. EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions - Europol, accessed April 24, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EFIPPP_Practica

l_Guide.pdf
81. Europol Analysis Projects, accessed April 24, 2025, https://www.europol.europa.eu/operations-services-innovation/europol-analysis-projects
82. European Financial and Economic Crime Centre - EFECC - Europol, accessed April 24, 2025, https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc
83. IOSCO, accessed April 24, 2025, https://www.iosco.org/
84. International Organization of Securities Commissions (IOSCO), accessed April 24, 2025, https://www.belizefsc.org.bz/international-organization-of-securities-commissions/
85. International Organization of Securities Commissions (IOSCO) - IAS Plus, accessed April 24, 2025, https://www.iasplus.com/en/resources/global-organisations/iosco
86. IOSCO Objectives and Principles of Securities Regulation, accessed April 24, 2025, https://www.iosco.org/library/pubdocs/pdf/ioscopd561.pdf
87. Chargebacks Made Simple Guide | Mastercard, accessed April 24, 2025, https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/chargebacks-made-simple-guide.pdf
88. Chargeback Reason Codes, accessed April 24, 2025, https://www.chargebackgurus.com/chargeback-reason-codes
89. Explanation of the Chargeback Process & Flow - Kount, accessed April 24, 2025, https://kount.com/blog/explanation-chargeback-process-flow
90. Recover Funds Lost to Financial Fraud | Giambrone & Partners, accessed April 24, 2025, https://www.giambronelaw.com/site/servicesforindividuals/forex-litigation-lawyers/insights-recovery-of-funds-lost-in-financial-scams/
91. Legal Tools for Asset Recovery | Avenues to tackle cases involving recovery of stolen assets, accessed April 24, 2025, https://star.worldbank.org/focus-area/legal-tools-asset-recovery
92. Morgan & Morgan Investigating Binary Options Fraud - Business Trial Group, accessed April 24, 2025, https://www.businesstrialgroup.com/news/binary-options-fraud/
93. The Class Certification of Exchange-Listed Options in Securities Class-Action Litigation - Penn Carey Law: Legal Scholarship Repository, accessed April 24, 2025, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1725&context=jbl
94. Recovering Investments From a Ponzi Scheme in Canada - Roland Luo, accessed April 24, 2025, https://www.rolandlaw.ca/blog/recovering-investments-from-a-ponzi-scheme-tactics-and-lessons-learned/
95. Recovering From Fraud | CFTC, accessed April 24, 2025, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/recoveringfromloss

es.html
96. Fraud Alerts - Treasury's Office of Inspector General, accessed April 24, 2025, https://oig.treasury.gov/fraud-alerts