

Fraud, Scams, and Deceptive Practices

Policy Rationale

We aim to protect users and businesses from being deceived out of their money, property or personal information. We achieve this by removing content and combatting behavior that purposefully employs deceptive means - such as wilful misrepresentation, stolen information and exaggerated claims - to either scam or defraud users and businesses, or to drive engagement. This includes content that seeks to coordinate or promote those activities using our services. We allow people to raise awareness and educate others as well as condemn these activities.

We do not allow:

Content that attempts to scam or defraud users and/or businesses by means of:

Loan Fraud and Scams

Content that:

- Offers loans requiring the user to pay an advance fee to obtain a loan.
- Offers loans with guarantee or near-guarantee of approval, either explicitly stated or implicitly understood based on context (such as claims to approve loan without asking for financial information).
- Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity and a bank or financial institution.

Gambling Fraud and Scams

Content that:

Offers real money gambling services (“Real money” is real-world currency that can be used to buy goods or services in the real world, including national currencies such as U.S. Dollars and virtual currencies such as Bitcoin):

- with a guarantee of winning.
- implying or admitting to have rigged the outcome of a game or match.
- soliciting people to enable match fixing or looking for help or tips on how to fix a match or game.

Social casino games that simulate gambling with no opportunity to win real money fall under our [Community Standard for Restricted Goods and Services](#).

Investment or Financial Fraud and Scams

Investment Opportunities. Content that:

- Offers investment opportunities where returns on investment are guaranteed or risk-free.
- Offers investment opportunities where returns on investment or compensation is partly or fully based on recruitment of others to participate in the scheme.
- Offers investment opportunities where the opportunity is of a “get-rich-quick” nature and/or claims that a small investment can be turned into a large amount.

Money/Cash Flip. Content that:

Offers to turn a certain sum of money into a larger one through flipping or trick or strategy involving explicit mentions of “cash flip,” “money flip,” or similar terminology.

Money Muling and Laundering Fraud and Scams

Money Muling. Content that:

- Offers or asks for money muling (causing victims to be unknowing participants in money laundering by offering money or share of profits in exchange for allowing others to use their bank accounts or transferring money on behalf of others).
- Offers or asks for money muling by offering employment to accept and transfer money to third parties using the victim’s bank account.

Money Laundering. Content that:

Requests, solicits, or offers to facilitate money laundering, which is an attempt to make illegally obtained money appear legitimate by disguising the origin of the money through a complex sequence of financial transactions, including through any of the following means:

- Seeking transfer of funds through SWIFT (Society for Worldwide Interbank Financial Telecommunications) or similar methods,
- Seeking or offering details on types of bank accounts available to support receipt or transfer of cash.

Inauthentic Identity Fraud and Scams

Content that:

Attempts to scam or defraud users by misrepresenting the identity of the poster or nature of a request:

- Charity Fraud and Scam, which are fraudulent requests for money or donations for charitable causes together with claims that the donation is urgent and includes information, such as bank accounts, where money can be sent.
- Romance Fraud and Scam, which are fraudulent attempts to establish online romantic relationships by seeking non-sexual companionship or relationship and offering or asking for money or its equivalent in exchange.
- Established Business/Entity Fraud and Scams, which involve falsely claiming to represent, or speak in the voice of, an established business or entity, in an attempt to scam or defraud.

Product or Reward Fraud and Scams

Government Grant Fraud and Scam. Content that:

Falsely offers money from government grants or any other governmental source of funding. We consider various signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it comes from a verified entity.

Tangible, Spiritual or Illuminati Fraud and Scam. Content that:

- Offers tangible rewards, such as money, goods, or services that have a monetary value including physical, digital and virtual currencies, and physical or digital goods and services for membership in or joining an association, cult, religious sect (for example, the Illuminati brotherhood).
- Offers tangible rewards for using black magic or spells or magical items (for example, spells, lucky charms, amulets, tokens, potions, magic wallet, etc.).

Insurance Fraud and Scams. Content that:

- Offers false, heavily discounted insurance with requests for an up-front fee (admin fee, or deposit, or otherwise).
- Offers false, heavily discounted insurance with promises of large savings on insurance compared to conventional insurance providers (at least 30% less).
- Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity and a bank or financial institution

Job Fraud and Scams. Content that:

- Offers jobs with an unclear or vague job description and get-rich-quick opportunities promising money with little time investment or effort.
- Offers jobs containing no job information, simply referencing job vacancies.
- Offers work from home but the job title implies the employee cannot WFH.
- Offers jobs with advance promises of salary.
- Offers guaranteed jobs.
- Offers jobs with a demand for an advance fee before the job is granted.
- Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity

Debt Relief and Credit Repair Fraud and Scam. Content that:

- Promises to delete or eliminate or reduce debt by a particular amount in a set period of time.
- Promises to stop or delete all debt collections or lawsuits.
- Promises to forgive or cancel debt through "new government program" or change in law or equivalent statement.
- Promises to delete or remove credit information from credit reports or create new "credit identity".
- Note: We also look for other signals to determine an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity and a bank or financial institution

Giveaway Fraud and Scam. Content that:

Offers a guaranteed reward of real money in exchange for users needing to:

- Register at an off-site link.
- Share Personal Identifiable Information (PII) or Other Personal Information.
- Contact off-platform or on-platform via private message.
- Take no action.

Advance Fee Fraud and Scam. Content that:

Falsely promises money in exchange for an up-front fee/wire transfer/payment.

Fake Documents Fraud and Scams

Fake or Forged Documents. Content that:

- Offers solicitation, creation, sale, purchase or trade of fake or forged documents.
- Offers sale of visas or green cards.
- Guarantees visa or green card approval.
- Enables users to get visa approvals without fulfilling normal requirements.

Fake or Counterfeit Currency. Content that:

Offers sale, purchase or trade of fake or counterfeit currency, except board-game currency (e.g., Monopoly money) if there is clear context that it is for board-game purposes.

Fake or Counterfeit Vouchers. Content that:

- Offers sharing, sale, purchase or trade of fake or counterfeit vouchers.
- Admits to, promotes, or solicits the use of physical or digital coupons or vouchers to achieve atypical pricing by either:
 - using coupons or vouchers to purchase items those coupons or vouchers are not intended for; or
 - by using expired coupons or vouchers.

Fake or forged educational and professional certificates. Content that:

Offers sale, purchase or trade of fake or forged educational and professional certificates.

Stolen Information, Goods or Services Fraud and Scam

Carding Fraud and Scam. Content that:

Involves buying, selling or trading of stolen credit cards or other financial instruments that can be used for unauthorized purchases (also known as "carding").

PII Fraud and Scam. Content that:

Offers buying, selling or trading of Personal Identifiable Information (PII) or Other Personal Information except if it belongs to a fictional character.

Fake Review Fraud and Scam. Content that:

- Calls for buying, selling or trading of product reviews/ratings.
- Implicitly or explicitly incentivises users to provide reviews in exchange for discounts, refunds or free items.

Subscription Fraud and Scam. Content that:

- Offers buying, selling or trading of credentials for subscription services (login credentials to online services which require a recurring payment at regular intervals) by making references to a paid online service, either by naming it or by sharing its logo.
- Note: We also look for other signals to determine if an entity is posting legitimate, non-fraudulent content, such as when it is a verified entity and a bank or financial institution.

Cheating Fraud and Scam. Content that:

Involves sharing, selling, trading, or buying of:

- future exam papers or answer sheets.
- Products or services that enable cheating in exams.
- Products or services that enable passing drug tests in an unauthorized manner

Unauthorized Use of Devices Fraud and Scam

Device Manipulation Fraud and Scam. Content that

- Calls for buying, selling, trading or sharing of any manipulated, altered, or fake measurement devices.
- Admits to, promotes or solicits use of physical manipulation of devices to achieve inaccurate pricing.

Digital Content Fraud and Scam. Content that

Offers or asks for products that facilitate or encourage access to digital content in an unauthorized manner. These include but are not limited to: augmented set top boxes, fully loaded/KODI installed boxes and KODI services.

Deceptive and Misleading Practices

Misleading Health Practices. Content that

Promotes false or misleading health claims or guarantees in a weight loss context by employing click-bait tactics, such as the use of sensational language that make exaggerated or extreme claims

For the following content, we limit the ability to view the content to adults, ages 18 and older:

Content that

Promises specific weight-loss results in specific time with no qualifying or disclaimer language.

Notwithstanding the above, we do not prohibit content that condemns, raises awareness of or educates others about fraud and scams, without either revealing sensitive information or promoting fraud or scams

For the following Community Standards, we require additional information and/or context to enforce:

We may remove content:

- Involving fraud/scam that have been reported by a trusted entity.
- Related to bribery or embezzlement.
- That offers vaccines in an attempt to scam or defraud users.
- That attempts to establish a fake persona, pretends to be a famous person, or makes unauthorized use of an image of a famous person in an attempt to scam or defraud.
- That offers or asks for products or services designed to facilitate the surreptitious viewing or recording of individuals, e.g., spy cams, mobile phone trackers (including those that allow tracing unknown phone numbers), or other hidden surveillance equipment.
- That offers litigant recruitment opportunities for people to participate in class action lawsuits by impersonating a government entity or a news outlet, by using sensationalist language, or by using exaggerated claims.
- That offers subscription services that prompt users to enter Personal Information.
- We do not allow entities to participate in or claim to engage in organized Fraud or Scam behavior, including the use of multiple accounts on our services in concert to perpetrate fraudulent behaviors.

In certain cases, we allow content that may otherwise violate the Community Standards when it is determined that the content is satirical. Content will only be allowed if the violating elements of the content are being satirized or attributed to something or someone else in order to mock or criticize them.