

Scam Prevention Notice

V01/2026



PURE DMA TRADING
GUARANTEED
STP EXECUTION



Scam Prevention Information

Hogg Capital Investments Limited is working hard to fight cybercrime and fraud, to keep you as safe as possible. We use transaction monitoring and screening tools to identify and prevent fraud and money laundering. Below are answers to a few common questions about fraud and how you can prevent it:

What is a scam?

A scam is where you're tricked into sending money or digital assets (i.e. cryptocurrencies) to a scammer, who then steals the money or digital assets. Scammers might impersonate people and organisations you trust, using documents, emails, phone calls, and texts that seem genuine. They may ask you to download apps or sign up for specialized investment websites [such as ourselves]. Many victims are contacted by scammers through investment, trading or learning chat groups on WhatsApp, Telegram or Signal. Many scams promise overly high investment returns or claim to facilitate access to investment opportunities not available to the general public.

I've been scammed and the transaction details mention Hogg Capital Investments Limited. What should I do?

If you believe you have been affected by fraud or a scam, we strongly recommend that you notify your bank or financial institution immediately. They may be able to recall the payment. You should also report any suspected fraud or scam to your local law enforcement agency or directly to us. If you do want to report the suspected fraud to us, please contact us at support@tier1fx.com.

I've been contacted by someone claiming to represent Hogg Capital Investments Limited. How do I know this communication is legitimate?

Check the source: Legitimate communications from Hogg Capital Investments Limited will only come from our official email addresses: support@tier1fx.com, applications@tier1fx.com, compliance@tier1fx.com or your Account Manager's email address @tier1fx.com. We urge you to exercise caution and verify a sender's identity before responding to any communication claiming to be from us.

We will never ask you to:

- Disclose your password or one-time passcodes.
- Disclose full authentication credentials.
- Provide confidential information over social media platforms.
- Move funds to a "safe account".
- Transfer funds or assets for "verification purposes".

How do I spot a scam?

Scammers employ a range of tactics:

- **Creating urgency:** Pressuring you to act quickly, such as claiming an offer is limited or payment is needed immediately.
- **Promising high returns:** Offering unusually high or guaranteed profits, often linked to cryptocurrencies, stablecoins, AI, “algorithmic trading”, or other complex or trending products.
- **Pretending to be trusted people:** Impersonating banks, regulators, colleagues, friends, or real company employees.
- **Building trust over time:** Using social media, messaging apps, or group chats to form relationships before introducing investment opportunities or asking for money.
- **Using emotional manipulation:** Exploiting personal relationships (common in romance scams) by fabricating emergencies, hardships, or trust-based investment opportunities to encourage payments.
- **Exclusivity:** Claiming opportunities are “invite-only” or available only to a select few.
- **Looking professional:** Using polished websites, contracts, apps, or documents to appear legitimate.
- **Payment redirection:** Asking you to send funds to new or different accounts (often at short notice), sometimes claiming it is for security, efficiency, or compliance reasons.
- **Using complex language:** Overloading you with technical jargon or complex explanations (e.g. around trading strategies or crypto infrastructure) to sound credible and discourage questions.
- **Asking for more over time:** Encouraging increasingly larger payments over time, often by showing fake “profits” or returns at first.

How can you protect yourself from scams?

- **Be cautious:** Be wary of offers promising guaranteed profits or “get rich quick” opportunities.
- **Don’t rush:** If you feel pressured to act urgently, stop and verify the request independently before proceeding.
- **Check identities:** Research companies or individuals before sending any money. Look for public sources and reviews, and check email addresses, phone numbers, and website domains carefully for inconsistencies, misspellings, or anything suspicious.
- **Check licensing:** Confirm whether a firm is authorised by checking the local financial services register.
- **Protect personal information:** Don’t share personal details or identity documents with people you only know online.
- **Keep control of your accounts:** Never let someone else open or manage payment accounts or crypto wallets for you without proper verification.
- **Avoid remote access:** Do not install remote access software that gives strangers access and control over your device or financial accounts.
- **Known counterparties:** Be cautious when sending money or cryptocurrencies to individuals you have only met online, including through social media, messaging apps, or group chats.
- **Payment requests:** Be cautious of unexpected or urgent requests for money or changes to payment details, especially if they involve changes to usual payment details or methods.
- **Look out for recovery scams:** If you are scammed, scammers may pretend they can recover lost funds or digital assets if you pay them upfront.
- **Be aware of emotional pressure:** Romance, emergencies, or personal hardship may be used as a way to influence your decisions.
- **Use secure communication:** Don’t click on links or downloading attachments in unexpected messages, particularly those asking for payments, personal information, or login details.
- **Ask for advice:** If in doubt, speak to someone you trust or contact the organisation directly using verified contact details.
- **Review transactions carefully:** Double check payment details carefully before sending funds, especially for first-time or high



Nu Bis Centre
Mosta Road, Lija
LJA9012, Malta
+356 2327 3000 | support@tier1fx.com
www.tier1fx.com

Tier1FX represents the branded offering of the online brokerage division of Hogg Capital Investments Limited which is a fully licensed Class II Investment Firm (registration number C 18954) authorized under the Investment Services Act, regulated in Malta by the Malta Financial Services Authority (MFSA) and located at Nu Bis Centre, Mosta Road, Lija LJA9012, Malta. Our authorization may be viewed here: <https://www.mfsa.mt/financial-services-register/>