CAMBRIDGE

PROTECT YOURSELF
FROM SCAMS AND FRAUD

Fraud and scams affect investors of all ages and experience levels. Scammers often appear professional, urgent, and convincing. This guide is designed to help you recognize potential warning signs and protect your assets and personal information.

WARNING SIGNS THAT MAY INDICATE FRAUD

- Promise of high returns with little or no risk
- Inconsistent or confusing explanations of how the investment works
- Refusal to provide written documentation
- Pressure to keep the opportunity confidential
- Request for personal or account information
- Request to make payment via cash or cryptocurrency

COMMON CHARACTERISTICS OF SCAMS

Be cautious if you encounter any of the following:

- "Guaranteed" or low risk, high return: No legitimate investment can guarantee profits or eliminate risk. Claims of "risk free," "can't miss," or "guaranteed returns" are major warning signs.
- Pressure to act quickly: Scammers often create a false sense of urgency, telling you an opportunity is available "for a limited time only" or that you must act immediately
- Unsolicited offers: Unexpected investment offers via phone calls, texts, emails, social media, or messaging apps should be treated with caution, especially if you do not know the sender
- Requests for unusual payments: Be wary of requests to send money via wire transfer, cash, cryptocurrency, prepaid cards, or peer-to-peer payment apps (such as Venmo or CashApp)

STEPS TO PROTECT YOURSELF

IF YOU SUSPECT FRAUD OR A SCAM, IMMEDIATELY:

- Stop all communication with the suspected scammer
- Put a stop to sending additional funds
- Contact your financial professional
- Monitor your accounts for unusual activity
- Consider reporting the activity to the appropriate authorities

AUTHORITIES

- Securities Exchange Commission
- FBI Internet Crime Complaint Center
- Federal Trade Commission
- Your state securities regulator
- Your state attorney general

Scammers rely on urgency, trust, and emotion. Taking time to verify, asking questions, and staying informed are your best defenses. When in doubt—pause and ask.

Security Checklist:

- ☐ Enable Multi-factor Authentication (MFA) on all financial accounts
- ☐ Use a trusted password generator and manager
- ☐ Do not reuse passwords
- ☐ Keep devices updated
- ☐ Avoid public Wi-Fi for financial activity

If you have concerns or questions about an investment opportunity, reach out to your financial professional before taking action.

CAMBRIDGE