

# Common Scams and How to Protect Yourself

**Losses from fraud continue to grow as criminals and the technology they use become increasingly sophisticated. Be on the lookout for these common scams to help keep your assets safe:**

## Merchant / Vendor Scams

Fraudsters impersonate trusted sources and target emailed payment instructions from organizations or people you want to pay.

- Protect yourself: Always verbally confirm the bank name, account name and account number with the recipient over the phone on an independently sourced number, not one that has been received over email.
- Carefully examine email addresses to detect “spoofed” emails, (e.g., fraudteam@goldman.com vs. fraudteam@go1dman.com).

## Impersonation

Fraudsters claim to be police officers, bank representatives or other trusted officials and say you need to send money immediately to prevent prosecution or penalties.

- Protect yourself: Hang up and call on an independently sourced phone number to confirm if requests are legitimate.

## Keep in Mind

Fraudsters may call you and attempt to impersonate friends or family members in an emergency situation and ask you to send money urgently.

Fraudsters can spoof phone numbers to look like they are calling from a known party’s actual phone number, even when they are calling from another country.

Be cautious of unsolicited outreach for investment opportunities or personal information—even if it seems to be coming from a known or reputable company.

If you are unsure regarding the legitimacy of an incoming call, hangup and call back on an independently sourced phone number to confirm if requests are legitimate.

Goldman Sachs will never ask you to join social media or messaging groups to provide investment advice or opportunities.

## Payment Scams

Fraudsters promise returns on transactions that are 'too good to be true,' typically involve crypto currency, and are commonly solicited by someone you have never met in person.

- Protect yourself: Talk to your Goldman Sachs team about any money movement prior to initiation. Thoroughly research potential payees or merchants and don't be pressured to act quickly. Don't assume opportunities advertised on social media are legitimate.

## Brand Scams

Fraudsters can generate fake emails, websites, and even mobile applications designed to impersonate our Brand to request activity outside of secure channels.

- Protect yourself: Always verify the activity as fraudsters may leverage artificial intelligence to generate well written text or designs. Carefully examine websites and applications. Talk to your Goldman Sachs team about any concerns.

## What can you do?

### Be Proactive

Don't use email to send or store sensitive information, such as usernames, passwords, PINs, bank account numbers and personal identification information. Use different passwords for all email accounts and websites.

Be sure to thoroughly research all potential investments before sending a payment, and don't be pressured to act quickly.

For people who you speak with frequently, consider leveraging a codeword you can ask for to verify identity in cases where the conversation feels suspect.

Enable multi-factor authentication for email, phone provider, financial and social media websites.

### Be Vigilant

Incoming calls displaying the police, your bank or any recognized organization aren't always legitimate.

Legitimate parties should be comfortable with you hanging up and calling back on an independently sourced phone number.

### Be Aware

The widespread availability of generative AI tools makes it easier for cyber criminals to create sophisticated and hard-to-detect scams intended to defraud potential victims.

If you are ever uncertain regarding the legitimacy of a communication from Goldman Sachs Custody Solutions, please reach out to your Goldman Sachs Custody Solutions team. Goldman Sachs will always reach out using firm approved messaging systems to connect with clients and emails will always be sent from the @gs.com domain