# SCAM AWARENESS AND FRAUD PREVENTION

SHARPAY is committed to protecting its customers from fraud and financial crime. Payment scams are increasingly common, and customers should remain cautious when receiving requests to send funds or share sensitive information.

## Common Fraud Techniques

Fraudsters may attempt to deceive customers using various methods, including:
**Phishing, Smishing, and Vishing** – fraudulent emails, text messages, or phone calls designed to obtain sensitive information such as passwords or authentication codes.
**Spoofing** – fake websites, email addresses, or phone numbers that imitate legitimate organizations.
**Urgent Payment Requests** – messages that pressure you to send money quickly or bypass normal verification procedures.
**Investment or Technical Support Scams** – requests to transfer funds for fake investment opportunities or to resolve alleged security issues.

## How to Protect Yourself

Customers can reduce the risk of fraud by following these precautions:

- Verify the identity of the person or business requesting payment.
- Never share passwords, authentication codes, or other confidential information.
- Carefully review payment details before confirming any transaction.
- Be cautious of unsolicited requests that create urgency or pressure.
- Do not send funds to individuals or organizations you do not know or trust.

Customers are responsible for maintaining the security of their account credentials and payment authentication methods. This includes protecting passwords, authentication codes, and any other security information associated with their SHARPAY account.

SHARPAY will **never ask you to transfer funds to a "safe account"** or request confidential security credentials.

## Unauthorized Transactions and Reporting

If a customer believes that a transaction has been executed without authorization or suspects fraudulent activity, they should notify SHARPAY immediately.

Upon receiving such notification, SHARPAY may review the transaction, implement appropriate security measures, and cooperate with financial institutions or relevant authorities where necessary.

Customers are encouraged to report suspicious activity as soon as possible, as delays in reporting may reduce the likelihood that a transaction can be investigated or mitigated.

Please note that once a payment has been executed, it may not always be possible to reverse the transaction. Customers should therefore carefully verify all payment details before confirming a transfer.