Fraud and Security Policy

Mosta · Last updated 2026-11-11

1. Introduction

1.1 Purpose. This Fraud and Security Policy ("Policy") describes the measures the licensed companies maintain to prevent fraud, protect your account, and ensure the security of the Mosta platform. The licensed companies are the companies identified on the Licensing page at https://legal.mosta.io/v4/licensing. "Mosta" is the trade name of the website and platform at https://mosta.io, under which the licensed companies provide their services. This Policy also provides guidance on how you can protect yourself and report suspicious activity.

1.2 Scope. This Policy applies to all users of the Platform and covers fraud prevention, cybersecurity controls, identity verification, incident management, and user security responsibilities.

1.3 Commitment. We are committed to maintaining robust security controls to protect your account, personal information, and funds from unauthorized access, fraud, and cyber threats.

2. Our Security Measures

2.1 Identity Verification. We implement comprehensive identity verification procedures, including:

- Document verification using government-issued identification;
- Biometric verification where applicable;
- Address verification;
- Enhanced due diligence for higher-risk accounts;
- Ongoing monitoring and periodic re-verification.

2.2 Account Security. We protect your account through:

Multi-Factor Authentication (MFA)	Required for sensitive actions including fund transfers, withdrawals, beneficiary changes, and security setting modifications
Encryption	All data is encrypted in transit and at rest using industry-standard protocols
Session Management	Automatic session timeouts and secure session handling
Access Controls	Role-based access and principle of least privilege

2.3 Transaction Monitoring. We employ continuous monitoring to detect and prevent fraud: real-time transaction screening; behavioral analytics to identify unusual patterns; velocity checks and transaction limits; sanctions and watchlist screening; and automated alerts for suspicious activity.

2.4 Infrastructure Security. Our technical infrastructure is protected by firewalls and intrusion detection systems; regular security assessments and penetration testing; vulnerability management and patching; secure development practices; and 24/7 system monitoring.

3. Protecting Yourself from Fraud

3.1 Common Scams to Avoid. Be aware of these common fraud schemes:

Phishing	Fraudulent emails, texts, or calls impersonating Mosta or other legitimate organizations to steal your credentials or personal information. We will never ask for your password, MFA codes, or full payment details via email or phone.
Social Engineering	Manipulative tactics to trick you into revealing sensitive information or authorizing transactions. Scammers may create urgency, impersonate authority figures, or appeal to emotions.
Investment Scams	Promises of guaranteed returns, "get rich quick" schemes, or pressure to invest immediately. If it sounds too good to be true, it probably is.
Impersonation Scams	Fraudsters posing as Mosta employees, government officials, or technical support to gain access to your account.
Account Takeover	Criminals gaining unauthorized access to your account through stolen credentials, SIM swapping, or malware.
Authorized Push Payment Fraud	Being tricked into voluntarily sending money to a fraudster, often through romance scams, fake invoices, or impersonation.

3.2 How to Protect Yourself. Follow these security best practices.

Account security:

- Use a strong, unique password for your Mosta account;
- Enable multi-factor authentication (MFA);
- Never share your password, MFA codes, or security questions;
- Log out after each session, especially on shared devices;
- Regularly review your account activity and transaction history.

Communication safety:

- Verify the sender of any communication claiming to be from Mosta;
- Do not click links in unexpected emails or messages — go directly to mosta.io;
- Be suspicious of urgent requests for money or personal information;
- Contact us directly if you receive suspicious communications.

Device security:

- Keep your devices and software updated;
- Use antivirus and anti-malware software;
- Avoid using public Wi-Fi for financial transactions;
- Secure your email account with strong authentication.

Transaction safety:

- Verify recipient details before confirming any transaction;
- Be cautious of requests to send money to unfamiliar recipients;
- Take time to review — legitimate requests won't pressure you to act immediately;
- If you're unsure about a transaction, stop and verify independently.

4. Reporting Suspicious Activity

4.1 What to Report. Report immediately if you notice:

- Unauthorized transactions on your account;
- Login attempts or access you did not authorize;
- Changes to your account information you did not make;
- Suspicious emails, calls, or messages claiming to be from Mosta;
- Requests for your password, MFA codes, or sensitive information;
- Any other activity that seems unusual or concerning.

4.2 How to Report. Contact us immediately at support@mosta.io with the subject line "URGENT — Security/Fraud Report". When reporting, include your full name and account email; a description of the suspicious activity; the date and time of the incident; any relevant screenshots or transaction details; and actions you have already taken.

4.3 Our Response. When you report suspicious activity, we will acknowledge your report promptly; investigate the incident thoroughly; take appropriate action to secure your account; keep you informed of the investigation status; provide guidance on additional steps you should take; and report to authorities if required by law.

4.4 Account Freeze. If you believe your account has been compromised, request an immediate account freeze by contacting support@mosta.io with "URGENT — Account Freeze Request" in the subject line.

5. Incident Management

5.1 Security Incidents. We maintain documented incident management procedures to:

- Detect and respond to security incidents promptly;
- Contain and mitigate the impact of incidents;
- Investigate root causes;
- Implement corrective measures;
- Notify affected users and authorities as required.

5.2 Notification. If a security incident affects your personal information or account, we will notify you in accordance with applicable laws and regulations, providing information about the incident and recommended protective actions.

6. Cooperation with Law Enforcement

6.1 Reporting. We cooperate with law enforcement agencies investigating fraud and cybercrime. We may report suspicious activity to appropriate authorities without notice to you where permitted or required by law.

6.2 Preservation. We maintain records and may preserve evidence related to suspected fraud or security incidents for use in investigations and legal proceedings.

7. Security of the Services

7.1 Provider Security. The licensed companies maintain security and fraud-prevention measures for the financial services they provide. Where the licensed companies engage third-party custodians or other subcontractors, they require them to maintain security measures appropriate to their role and consistent with applicable regulatory requirements.

7.2 Your Responsibility. You are responsible for maintaining the security of your account and credentials and for following our security guidelines.

8. Limitation of Liability

8.1 User Responsibility. While we implement robust security measures, you are responsible for:

- Maintaining the security of your login credentials;
- Protecting your devices and email accounts;
- Reviewing transactions and reporting unauthorized activity promptly;
- Following the security guidance in this Policy.

8.2 Limitation. As set forth in our Terms and Conditions, we are not liable for losses resulting from your failure to safeguard your credentials, unauthorized access due to compromised authentication, phishing or social engineering attacks where you disclosed information, or transactions you authorized (even if induced by fraud by third parties).

9. Changes to This Policy

9.1 Modifications. We may update this Policy to reflect changes in security practices, threats, or regulatory requirements. Material changes will be communicated via email or Platform notification.

9.2 Version Control. We maintain version control and update logs for this Policy for at least five (5) years. Previous versions are available upon request to info@mosta.io.

10. Contact Information

Report Suspicious Activity or Security Concerns	support@mosta.io · mosta.io
Urgent Security Issues	support@mosta.io · Subject: URGENT — Security Issue
Legal and Compliance Inquiries	compliance@mosta.io

Remember: Mosta will never ask you to share your password, MFA codes, or send funds to "secure" your account.

If you receive such a request, it is fraudulent — report it immediately.