

Policy on Compensation for Unauthorized Transactions

RESPECT PAYMENT SERVICE Co., Ltd. (the “Company”) promptly investigates loss caused to customers by unauthorized use, fraudulent remittances, impersonation, account takeover or other fraud involving its funds transfer services. The Company determines whether and to what extent compensation is appropriate based on the customer’s responsibilities, the Company’s controls, the nature of the harm and other circumstances.

The Company attaches importance to protecting customers’ property, rights and interests and responds to fraud and compensation claims under the following policy.

1. Services Covered

This Policy covers unauthorized-use losses associated with the Company’s funds transfer services and the following related procedures:

- (1) Customer registration
- (2) Identity verification
- (3) Login and authentication
- (4) Changes to registered details and authentication information
- (5) Deposits
- (6) International remittances and other transfers
- (7) Cancellation, recall and refund
- (8) Other related service procedures

2. Unauthorized-Use Loss

For this Policy, unauthorized-use loss means damage arising when a third party improperly uses a customer’s account, authentication credentials, identity information, device or other means without the customer’s intention or valid authorization.

Such loss includes principally:

- (1) Unauthorized use of a customer ID or password
- (2) Unauthorized use of authentication codes or other credentials
- (3) Takeover of a customer device or account
- (4) Changes to registered details by impersonating the customer
- (5) Transfers made without the customer’s consent
- (6) Fraudulent transactions exploiting defects in the systems or administration of the Company or its contractors
- (7) Other fraudulent transactions not based on the customer’s intention

3. Transfers Induced by Third-Party Deception

Where a customer personally makes a transfer because of investment fraud, romance fraud, false billing, a fraudster impersonating a police officer, bank or Company employee, or other deception, the case is investigated separately from third-party account takeover.

The Company will not refuse to accept a report, investigate or provide possible fund-recovery assistance merely because the customer personally operated the transfer.

The availability and extent of compensation are determined case by case considering the fraud method, what the customer knew, warnings and confirmations displayed by the Company, transaction anomalies, detection, transaction holds and other circumstances.

4. Reporting a Loss

The Company endeavors to notify customers of important account activities so that unauthorized logins, transfers or changes can be identified early. Customers should promptly contact the Company about notifications they do not recognize.

Customers who detect unfamiliar logins, changes to registration details, deposits, remittances or other transactions should promptly contact the Company's customer support desk.

Upon receipt of a report, the Company may take the following steps as appropriate:

- (1) Temporarily suspend the customer's account
- (2) Invalidate login sessions
- (3) Change or reset authentication information
- (4) Check registered devices and contact information
- (5) Hold or stop remittances and other transactions
- (6) Request destination institutions or banks to stop or recover funds
- (7) Investigate related transactions and accounts
- (8) Advise the customer on preventing further harm
- (9) Take other steps necessary to limit the damage

5. Cooperation Requested from Customers

To investigate unauthorized-use losses and recover funds, the Company may reasonably request customers to:

- (1) Explain the events and when they became aware of them
- (2) Submit a fraud report and other documents
- (3) Provide identity-verification materials
- (4) Identify unfamiliar transactions
- (5) Provide relevant device, email, SMS, telephone and other records
- (6) Consult or file a report with the police
- (7) Contact banks and other related institutions
- (8) Change passwords or other authentication information
- (9) Provide other reasonable assistance for the investigation or recovery

The Company will not unduly delay necessary damage-prevention measures simply because the customer cannot immediately provide every requested document.

6. Investigation

When a customer reports unauthorized-use loss, the Company investigates the following as appropriate:

- (1) Registration and identity-verification circumstances
- (2) Login and authentication records
- (3) Devices, IP addresses and other technical data
- (4) Changes to registered or authentication details
- (5) Deposit and remittance histories
- (6) Destination and beneficiary information
- (7) Notifications sent to the customer
- (8) Detection and restrictions applied by the Company
- (9) Systems and administrative processes of the Company and its contractors
- (10) The customer's management of devices and credentials
- (11) Information received from banks, destination institutions, police or other parties
- (12) Other matters necessary for the compensation decision

7. Principles for Compensation Decisions

The Company assesses the following factors together and decides compensation and its extent on an individual basis:

- (1) Whether the transaction was authorized by the customer
- (2) The method and circumstances of unauthorized use
- (3) The Company's identity verification and authentication
- (4) The Company's fraud detection, customer notification and transaction controls
- (5) Defects in systems or processing by the Company or contractors
- (6) The customer's management of devices, credentials and registered information
- (7) The timeliness of the customer's report after becoming aware of the loss
- (8) The customer's cooperation to prevent further loss and assist the investigation
- (9) Fraud, coercion or other conduct by third parties
- (10) Funds recovered
- (11) Terms of use and other contractual conditions
- (12) Applicable law and regulatory requirements
- (13) Fairness and consistency with comparable previous cases
- (14) Other circumstances relevant to the compensation decision

8. Circumstances Supporting Compensation

The Company considers full or partial compensation where any of the following circumstances is found:

- (1) The transaction was unauthorized and not intended by the customer
- (2) The Company or a contractor had deficiencies in identification, authentication, systems or transaction processing
- (3) The Company detected or reasonably should have detected fraud but failed to take necessary steps
- (4) The Company's customer notifications or transaction restrictions were defective
- (5) No serious intentional wrongdoing or negligence by the customer is established
- (6) Compensation is otherwise appropriate for customer protection

9. Circumstances Limiting or Excluding Compensation

The Company may limit or refuse compensation, taking into account the causal connection between the following circumstances and the loss and the degree of responsibility:

- (1) The customer committed the unauthorized use or colluded with a third party
- (2) The customer knowingly made false statements or submitted false documents
- (3) The customer sought compensation fraudulently
- (4) The customer intentionally disclosed credentials to a third party despite recognizing the risk of misuse
- (5) The loss increased because the customer unreasonably disregarded specific protective measures advised by the Company
- (6) The loss increased because the customer unreasonably and substantially delayed reporting after becoming aware of misuse
- (7) The customer has already been compensated by another party for the same loss
- (8) Other circumstances establishing a clear causal connection between the loss and intentional conduct or gross negligence by the customer

Some negligence by the customer does not automatically result in complete denial of compensation.

The Company also considers the customer's age, disability, language, method of deception and any deficiencies in the Company's controls.

10. Amount of Compensation

The Company generally calculates compensation taking into account:

- (1) Amounts transferred or processed without authorization
- (2) Fees directly incurred by the customer due to the unauthorized use
- (3) Amounts recovered by cancellation, recall, return or other means
- (4) Amounts reimbursed by third parties or insurance
- (5) Other loss directly caused by unauthorized use

Indirect loss, lost profit, emotional distress and other damage are assessed case by case in light of causation, Company responsibility, applicable law and the Terms.

11. Recovery of Funds

Where funds from unauthorized use may remain with a bank, remittance destination, overseas partner or another institution, the Company will, to the extent possible and even before a compensation decision, take measures including:

- (1) Transaction suspension
- (2) Cancellation
- (3) Recall
- (4) Requests for return of funds
- (5) Requests for assistance from relevant banks or others
- (6) Cooperation with police and other agencies

Recovered amounts are taken into account in determining compensation.

12. Communications Pending Decision

If investigation or determination of compensation takes time, the Company informs customers of receipt of the claim, investigation progress, additional materials required and expected next contact.

The Company will not leave a customer without contact for an unreasonable period simply because an investigation remains ongoing.

13. Notification of Compensation Decision

The Company generally notifies the customer of its decision and the amount in a traceable form.

The notice may include as appropriate:

- (1) Transactions investigated
- (2) Investigation findings
- (3) Whether compensation will be paid
- (4) Amount and calculation
- (5) Payment method and expected payment date
- (6) Reasons for restricting or denying compensation
- (7) Additional procedures required
- (8) Inquiry and complaint contact points
- (9) Financial ADR or other dispute-resolution avenues

14. Payment of Compensation

After required approvals, the Company pays compensation within a reasonable period, generally to a bank account in the customer's own name or by another approved method.

The Company verifies the eligible recipient, amount, payment destination and absence of double payment before disbursement.

Where false statements, fraudulent claims or duplicate reimbursement come to light after payment, the Company may seek repayment under applicable laws and Terms.

15. Handling of Personal Information

Personal information obtained in investigating and compensating unauthorized use is used for:

- (1) Identity verification
- (2) Investigating the damage and facts
- (3) Stopping misuse and preventing further harm
- (4) Recovering funds
- (5) Compensation assessment and payment
- (6) Coordination with police, banks, destinations and other partners
- (7) Root-cause analysis and preventing recurrence
- (8) Mandatory reports and responses to lawful inquiries

The Company manages this information under applicable law and its Privacy Policy.

16. Cooperation with Police and Others

In the case of suspected crime, the Company may request that customers consult or file a report with the police.

The Company works with police, financial institutions, funds transfer providers, destinations, overseas partners, contractors and others within the bounds of law and as needed to protect customers.

17. Complaints and Appeals

Questions, complaints or appeals relating to compensation decisions may be submitted to the Company's inquiry desk.

The Company reassesses relevant facts and decisions as needed.

Where discussion with the Company does not resolve the matter, customers may use financial ADR or other external dispute-resolution mechanisms through the Japan Payment Service Association and other bodies.

18. Contact Desk

The Company publishes contact details for unauthorized-use reports, compensation inquiries and complaints on its website or by other appropriate means.

Published contact details may include:

- (1) Name of inquiry desk
- (2) Telephone number
- (3) Email address or inquiry form
- (4) Service hours
- (5) Emergency contact methods
- (6) Other information necessary for contacting the Company

Details subject to change, such as address, telephone number or hours, are kept on the Company website or contact pages, rather than in this Policy.

19. Fraud Prevention

The Company implements appropriate risk-based measures to prevent unauthorized-use losses, including:

- (1) Identity verification
- (2) Authentication and account management
- (3) Detection of suspicious logins or transactions
- (4) Transaction amount and frequency limits
- (5) Holds and additional checks on high-risk transactions
- (6) Customer transaction notifications
- (7) Customer warnings and alerts
- (8) Preservation of logs and evidence
- (9) Cooperation with contractors, banks and remittance destinations
- (10) Staff education and training
- (11) Analysis of fraud incidents and improvement of controls

20. Customer Precautions

To help prevent unauthorized-use losses, customers should:

- (1) Never disclose IDs, passwords or authentication codes to third parties
- (2) Avoid reusing passwords across multiple services
- (3) Beware of suspicious emails, SMS, calls and websites impersonating the Company
- (4) Avoid opening suspicious links or attachments
- (5) Verify the recipient and purpose before making transfers at the direction of a third party
- (6) Promptly inform the Company if a device is lost
- (7) Keep registration and contact information current
- (8) Promptly report unfamiliar transactions or notifications

The Company will never request a customer's complete password or authentication code by telephone, email or SMS.

21. Relationship to Internal Policies

Reporting, initial response, investigation, compensation decisions, authorization, payment, recovery, root-cause analysis and records are governed by Internal Policy 13-01, Unauthorized Use and Compensation Management Regulations.

Complaints and disputes are governed by Internal Policy 7-01, Complaints, Financial ADR and Dispute Resolution Management Regulations, and Manual 7-02, Complaints and Financial ADR Procedures.

Cases classified as incidents or misconduct are handled under Internal Policy 5-01, Incident and Misconduct Management and Response Regulations.

22. Publication

The Company publishes this Policy on its website or through other appropriate means.

23. Amendments

Adoption, material amendment or repeal of this Policy requires board approval.

Minor changes not altering its substance, including adjustments to contact desks or details, may be approved by the representative director or compliance officer.

24. Superseded Policies

Former Policy 20-6, Policy on Compensation for Unauthorized Use in International Remittance Services (Public Version), is repealed from the effective date of this Policy.

The parts of former Policy 17-2, Policy on Compensation for Unauthorized Use in International Remittance Services, intended for public disclosure are consolidated into this Policy.

Former versions are retained with amendment, consolidation and comparison records.

Adoption and Revision History

Established: January 11, 2017

Revised: July 10, 2026

Revised: July 17, 2026

Consolidated revision: July 21, 2026