HIGHBLOCK LIMITED

Compliant Handling Procedure

Version: 1.0
Date: [2024.02.05]

Version Control

Policy Owner	Customer Service Team
Policy Approver	COO
Date for Next Review	Before 2025.02.05

Version	Approval Date	Effective Date	Description of Change	Author
1.0			**First draft**	Customer Service Team

Table of Contents

Version Control 1
Table of Contents 2
1. Complaint management 3
    1.1 Complaint Management Purpose 3
    1.2 Complaint Management Channel 3
    1.3 Customer Response Guide 4
    1.4 Complaint Management Tools 4
2. Compliant Response 4
    2.1 Complaint Receipt 4
    2.2 Complaint Handling 5
    2.3 Complaint Management 5
3. Complaint Handling Procedure 5
4. Similarly receiving, telecommunications and financial fraud, illegal marketing, and other illegal behavior response methods 13
    4.1 Classification of unlawful acts 13
    4.2 The reporting process for victims of unlawful acts 14
    4.3 Company Response 15
    4.4 Procedures for refunding the amount of money victimized by telecommunication and financial fraud (telephone fraud) 17
    4.5 Failure to reach an agreement between the account holder (member) and the victim 19
5. Wireline Complaint Response (Protecting Customer Service Personnel) 20
    5.1 If the customer does not hang up without accepting the guidelines and persistent pestering: 20
    5.2 If a customer uses inappropriate language that includes swearing or sexual harassment: 20
    5.3 If the customer asks for the call to be transferred to the highest responsible person or asks for contact information: 20
    5.4 If a customer persists in using rude language or is a nuisance to our work: 20
Schedules 21
    Schedule 1: 21
    Schedule 2: 22

1. Complaint management

1.1 Complaint Management Purpose

The main purpose of complaint management is to ensure customer satisfaction while improving and maintaining the quality of the organization's services. The objectives of complaint management include:

1.1.1 Customer Feedback: This helps the organization to understand the needs of its customers. This feedback can guide product improvements and business strategies.

1.1.2 Customer Satisfaction: Ensuring that customer issues are handled appropriately by proactively addressing and resolving complaints to increase customer satisfaction. Customer trust can be increased, and customer churn can be reduced by resolving customer difficulties.

1.1.3 Problem-solving: The purpose of complaint management is to identify and solve problems related to the organization's products or services. Complaint handling allows for timely correction of errors, improvement of processes, and prevention of recurrence of similar problems.

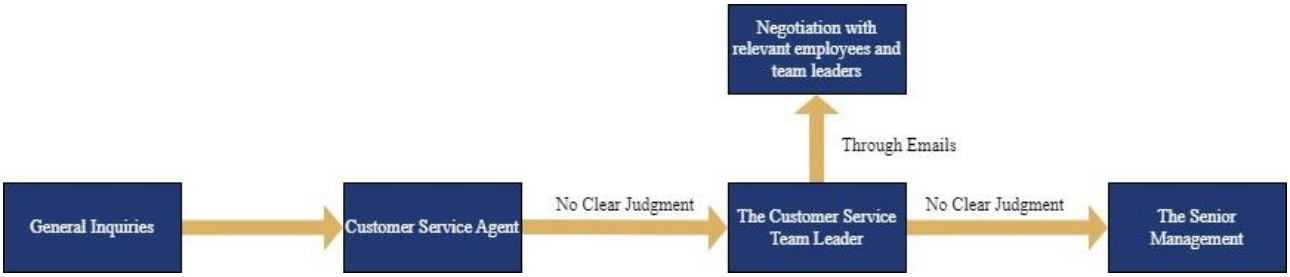
1.1.4 Continuous Improvement: By analysing complaint data, organizations can identify potential problems and improve business operations, product or service quality. This helps to improve organizational performance and efficiency.

1.1.5 Maintaining Reputation: Handling complaints proactively helps to maintain the organization's reputation. If complaints are not handled appropriately, they can damage a brand's reputation. Conversely, handling complaints properly builds trust and a positive brand image.

1.2 Complaint Management Channel

1.2.1 Complaint management channels include four methods: "telephone, online chat, online inquiries, and offline inquiries", the customer service center of the website provides guidelines and FAQ (Frequently Asked Questions) to explain in detail how to use each of the complaint channels and guidelines for inquiring about the contents.

1.2.2 Complaints are categorized into three types: "general inquiries, crime and hacking related, and advice". If they fall into the last category, other inquiries are prioritized and regularly collated for discussion at meetings.



1.3 Customer Response Guide

1.3.1 Each customer service agent should refer to this Procedure when handling complaints and should consult with the customer service supervisor in cases where his/her judgment is not clear. The customer service supervisor should consult with senior management in cases where his/her judgment is not clear or communicate via e-mail if consultation with other departments is required.

☞ Contact details

- Head of Risk Management Department
- Head of Operation Department
- Head of Information Technology Department
- Head of Legal Team
- Head of AML Team

1.4 Complaint Management Tools

1.4.1 Each customer service agent should use internal communication tools to share complaint issues so that customer service supervisors can conduct regular reviews to avoid giving incorrect responses and handling.

Customer service supervisors should summarize frequent complaints and important issues, share them with relevant departments regularly (e.g., weekly), and consider incorporating them into improvement plans for the complaint handling procedure. The basic principle is to use emails to share information and use meetings to conduct discussion.

2. Compliant Response

2.1 Complaint Receipt

2.1.1 Complaints are categorized into objection applications, appeals, suggestions, and inquiry acts.

2.1.2 Complaints can be received by telephone, online chat, e-mail, and through external organizations. The "Customer Service" -> "User Guide" -> "User Handbook" on the website explains in detail how to use the complaint channels and the contents of common complaints.

2.1.3 Except for simple suggestions and inquiries, all complaints are to be received in writing and records kept in accordance with the form attached to this Procedure.

2.2 Complaint Handling

2.2.1 The members of the Customer Service Team should refer to this Procedure for complaint receipt response, and if the judgment is not clear, they should discuss it with the customer service team leader.

2.2.2 The Customer Service Team Leader will need to consult with the relevant employees and team leaders when handling complaints, in which case email should be used for communication.

2.3 Complaint Management

2.3.1 The members of the Customer Service Team should record and manage complaints according to the forms in Schedule 1 and Schedule 2.

2.3.2 The Customer Service Team Leader regularly reviews the content of recorded complaints. If needed, helping team members improve their complaint handling skills through customer service team training.

2.3.3 The Customer Service Team Leader enhances the complaint management system by summarizing repetitive complaints and significant matters and sharing them with relevant teams regularly.

3. Complaint Handling Procedure

3.1 When a customer is suspected to have been subjected to criminal acts such as hacking, phishing or SMS fraud

3.1.1 When customer service agents receive a customer's suspicion that he or she has suffered a criminal act such as hacking, they shall guide the customer to report the case to a law enforcement agency, and after confirming the identity of the customer, request the freezing of the customer's account through the customer service supervisor.

3.1.2 If the customer is only suspicious and no actual legal proceedings are underway, the customer may request that the freeze be lifted; in the case of ongoing legal proceedings, the following guidelines can be used to lift the freeze.

a) Stage 1 guide: "If you need to freeze your account, please do so after your identity has been confirmed. In the meantime, please report the case to law enforcement agencies immediately.

b) Identification:

i. Confirmation of customer information: "Name, date of birth, unique identification number (UID), cell phone number, email address"

ii. If the cell phone number or email address provided by the customer does not match the registered information, customer service agents shall reconfirm the customer's information.

c) Stage 2 guide, "According to the internal process, we will process a freeze, please report to the law enforcement agency in the meantime and wait for the process."

d) Opinion of Freeze Request: After confirming the identity of the customer, the Customer Service Team Leader will report to the Senior Management and request to freeze the customer's account.

e) Notification after Freeze: After confirming the freeze request and completing the processing, the customer is notified of the freeze by phone or e-mail.

f) Unfreezing Process:

i. If the customer is only suspicious and no actual legal proceedings are underway, it is possible to request an unfreezing.

ii. The process of unfreezing is the same as freezing, but at the beginning, it is necessary to confirm "name, date of birth, unique identification number (UID), cell phone number, email address, photo ID and photo of the person holding the ID card", and the process is the same thereafter. (Request for unfreezing from internal senior management → completion of unfreezing → notification to the customer by phone or e-mail)

iii. If it involves ongoing legal proceedings, it cannot be unfrozen at will until the matter is concluded.

Handling by "4. Similarly receiving, telecommunications and financial fraud, illegal marketing, and other illegal behavior response methods" (see Table 1).

< Table 1>

①. We will explain the limitations of handling victimization complaints made only by telephone, as it is often difficult to know exactly what the victimization is and who he or she is.
②. Customers are advised to report the victimization to the police and other law enforcement agencies immediately.
③. We recommend customers to change passwords to ensure the security of accounts.
④. If the customer wishes to freeze or stop the deposit and withdrawal to his/her account, do the following: Confirmation by the customer (name, date of birth, UID, cell phone number, e-mail address) Recording of the call that involves the wish to freeze or stop deposit and withdrawal to

the account

Submission of a request for voluntary freezing of the account

⑤. Measures such as freezing of the account or stopping deposit and withdrawal to the account shall be taken after approval by the customer service team leader.

⑥. Upon completion of measures such as freezing accounts or stopping deposit and withdrawal, the relevant content is communicated to the customer (by phone, SMS, e-mail, etc.).

⑦. Sending the relevant content to the Head of the Risk Management Department via internal email. In this case, the CC recipients include the following:

Executive Group Members

Head of Finance Department

Head of AML Team

Head of Security Team

Head of Legal Tea

3.2 Regarding objections to the cancellation of service contracts and restrictions on use

3.2.1 By Article 15 of the User Agreement, the Company has the right to terminate or dissolve the customer's contract for the use of the services, and the Member has the right to object to this.

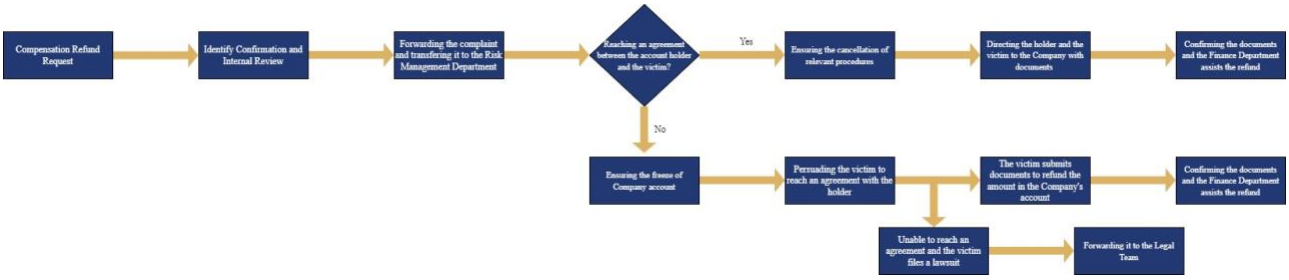
3.2.2 Applications for objections regarding the cancellation of service use contracts and restrictions on use will be accepted only within 15 days after the member receives the relevant notice. The Customer Service Team Leader will guide the complainant's complaint application by the provisions of Article 5, Article 6, and Article 7 in the following table (see Table 2).

< Table 2>

①. Objection requests for cancellation or restriction of the service use contract must be made within 15 days of the date of the notice, and members will be reminded of this.
②. Members can download the Complaint Application Form from "Customer Service" -> "User Guide" -> "User Handbook" -> "Complaint Application (Objection Application) Guide" on the website, fill in the form, and scan (1) your identification, (2) the Complaint Application Form, and (3) Relevant documents (supporting materials) and send them to verification@bitv.com. If a member is unable to access the website, he/she can also send the Application Form to the registered e-mail address.
③. Complaints will be handled within 7 working days from the date of receipt of the complaint.
④. If the complaint document needs to be supplemented, the complainant may be asked to do so. In such cases, the possible extension of the complaint processing time will be communicated.
⑤. Complaints are emailed to the following people and a committee is formed to consider them: Executive Group Members The AML Team The Risk Management Department The Legal Team Head of Finance Department Head of Security Team
⑥. After the Scrutiny Committee makes a decision and determines whether or not to accept the objection application, the Head of the Risk Management Department notifies the complainant of the outcome of the complaint (the outcome will be sent by post or email and the complainant will be notified of the outcome of the complaint by SMS).

⑦. If the objection application is accepted, the relevant member's account will resume normal use immediately.

3.3 Refund requests involving compensation of telecommunication and financial fraud (voice phishing)



3.3.1 The refund procedure for the compensation of telecommunication and financial fraud is established to refund compensations that are not subject to the claim elimination procedure of the financial supervisory authority and is a procedure carried out through an agreement between the fraudulent account nominee (member) and the victim of the fraud.

3.3.2 If the holder of the fraudulent account (member) and the victim reach an agreement to request the refund of the compensation, please handle the matter by the provisions of "4. Similarly receiving, telecommunications and financial fraud, illegal marketing, and other illegal behaviour response methods " (see Table 3).

< Table 3>

①. Performing member identification (name, date of birth, cell phone number, UID, email address). ②. If a complaint is received from a member about a compensation refund, it will be reviewed internally and then the detailed refund process will be explained. ③. You can download the Complaint Application Form from "Customer Service" -> "User Guide" -> "User Handbook" -> "Complaint Application (Objection Application) Guidelines" on the website, fill in the form, and scan (1) your identification, (2) Complaint Request Form and send it via verification@bitv.com. If a member does not have access to the website, he/she can also send the application form to the registered email address. ④. If a complaint is received about a compensation refund, please share this via email. Recipients will include the following: - Executive Group Members - The Finance Department - The AML Team - The Risk Management Department - The Security Team - The Legal Team ⑤. The Customer Service Team will handle the matter by "4. Similarly receiving,

telecommunications and financial fraud, illegal marketing, and other illegal behavior response methods" and will explain the process and other matters to the member.

3.4 When the Company is liable for damages caused by its negligence

3.4.1 The Company's internal compensation standards include compensation for additional handling fees due to withdrawal restrictions and financial losses due to exchange loopholes in the trading process. In the latter case, the judgment criteria may be ambiguous, so we will assist in the form of "post-confirmation notification". The final decision on compensation is made internally.

a) In the case of damages caused by the Company's negligence, a review of the user's compensation request is conducted after the member completes the submission of the complaint application form and related documents. (See Table 4)

b) The types of damages that the Company is currently dealing with include:

i. Compensation for additional handling fees due to failure to raise the deposit and withdrawal limits.

ii. Compensation for financial losses incurred by members in the course of trading as a result of the Company's technical problems".

< Table 4>

①. Members can download the Complaint Application Form from "Customer Service" -> "User Guide" -> "User Handbook" -> "Complaint Application (Objection Application) Guide" on the website, fill in the form, and scan (1) my identification, (2) the Complaint Application Form, and (3) Relevant documents (supporting materials) and send them to verification@bitv.com. If a member is unable to access the website, he/she can also send the application form to the registered email address.
②. Complaint handling will be completed within 7 working days from the day of receipt of the complaint.
③. If the complaint document needs to be supplemented, the complainant may be asked to do so. In such cases, the possible extension of the complaint processing time will be communicated.
④. Complaints are emailed to the following people and a committee is formed to consider them: - Executive Group Members - The AML Team - The Legal Team

- The Risk Management Department
- Head of the Finance Department
- Head of the Security Team

⑤. After the deliberation member makes a decision and determines whether or not the compensation is to be issued and after the amount of compensation has been paid, the Customer Service Team Leader notifies the complainant of the outcome of the complaint (sending the outcome of the complaint by post or email and notifying the outcome of the complaint by SMS).

3.4.2 In the case of delayed withdrawals, which are not compensable, guidance on the submission of evidence will be provided if there is a request for compensation for other losses, and the compensation decision will be made after submission.

a) Process Guide

Confirmation of personal information and relevant factual documentation is required. If you have followed the instructions to send us an e-mail, we will process it for you step by step.

b) Submission Form Guidelines

A form will be sent to the e-mail address you used to register your account, and you will need to respond as requested. (If the e-mail address is not registered, please register and send the form. Refer to Schedule 1 and Schedule 2)

c) Reporting to the senior management

After the Customer Service Team completes an initial review of the issue, reporting of all necessary information that has been collected.

*Reporting style

1. Receipt time
2. Person in charge of receipt
3. Reception contents (customer's reception contents)
4. Results of customer service audits (e.g., audits find good cause for reasonable compensation)

[Complaint handling procedure]

4. Similarly receiving, telecommunications and financial fraud, illegal marketing, and other illegal behavior response methods

4.1 Classification of unlawful acts

4.1.1 Similar illegal fund-raising practices

Under Hong Kong law, illegal fund-raising usually refers to the collection of funds from the public in an unauthorized or non-compliant manner, and such acts violate Hong Kong's laws and regulations. The following are some common features and explanations of illegal fund-raising practices:

a) Unauthorized fund-raising: Illegal fund-raising usually involves the collection of funds from the public without the authorization of the Hong Kong Securities and Futures Commission (SFC) or other relevant regulatory bodies.

b) Promises of high returns: Illegal fundraisers often promise investors high returns, but often fail to provide a legitimate investment plan or business model to support these promises.

c) Lack of regulation: Illegal fund-raisers are usually not regulated under the relevant Hong Kong legislation and may therefore lack transparency and oversight, leaving investors vulnerable to victimization.

d) Market manipulation: Some illegal fund-raising practices may involve market manipulation, dissemination of false information, or manipulation of stock prices to deceive investors.

e) Illegal activities: Illegal fund-raising may also involve other illegal activities such as fraud, money laundering, and tax evasion.

Illegal fund-raising practices may include the areas of stocks, futures, virtual assets, Internet investments, real estate, and others. Such conduct is a serious offense that can lead to criminal prosecution and legal sanction in the courts of Hong Kong.

4.1.2 Telecommunications and financial fraud

What is commonly referred to as telephone fraud, i.e. telecommunication and financial fraud, is a form of fraud in which the offender creates uneasiness by telephoning the victim and delivering threatening or false information, etc., and by doing so asks the victim to make a remittance. The following is a general explanation of telecommunication financial fraud under Hong Kong law:

a) Deception: Telecommunication and financial fraudsters usually employ various deceptive means, such as false identities or company names, false rewards or offers, threats or intimidation, to lure victims into providing personal information, bank account information, or funds.

b) False information: fraudsters may cause panic and confusion by claiming that the victim has outstanding debts, is involved in criminal activity, has won a lottery or sweepstakes, and needs urgent help.

c) Obtaining property: The main objective of telecommunication and financial fraud is to illegally obtain funds from the victim, usually through false investments, donations, transfers, remittances, or the purchase of false goods or services.

d) Unlawful means: Telecommunication and financial fraud is unlawful in that it involves the unlawful obtaining of funds or property by deception. These actions constitute a serious breach of Hong Kong's criminal laws.

e) Victim risk: Telecommunication and financial fraud can result in financial loss to the victim and, in serious cases, identity theft or other adverse consequences.

4.1.3 Ponzi scheme

A "Ponzi scheme" is a fraudulent scheme in which the fraudsters pays off early investors with money raised from new investors and continues to attract new investors. This type of scam needs to keep taking in new investors or it will collapse. A Ponzi scheme is one of the financial frauds that is widely recognized as an illegal activity to make a profit. Ponzi schemes deceive investors with high returns as bait so that they can gain monetary benefits and cause huge losses to people. Ponzi schemes include:

a) False promises: The mode of operation of a Ponzi scheme involves making false promises to investors, promising high returns or interest rates to entice them to invest. These promises are usually unrealistic and unattainable.

b) Source of funds: Ponzi schemes typically use funds from new investors to pay returns to early investors, rather than through actual profitable investment activity. This model can result in a system that constantly needs to attract new investors to pay returns to early investors.

c) Persistent deception: The key characteristic of a Ponzi scheme is the persistence of the deception. To maintain investor trust, the fraudsters will continue to provide false reports, fake accounts, and fake returns to convince investors that their money is safe.

d) Risk of collapse: A Ponzi scheme will eventually collapse either because not enough new investors enter or because of legal intervention. When the scheme collapses, most investors will suffer significant losses.

4.2 The reporting process for victims of unlawful acts

4.2.1 Victimized customers report to the police

a) Usually, most of the customers who have been harmed by similar illegal fund-raising practices,

telecommunication and financial frauds, Ponzi schemes, etc. will report their cases to the police or other law enforcement agencies.

b) After the police accept a report of victimization, if a search warrant needs to be executed, the customer sends the warrant and a law enforcement officer's certificate via the email provided at the bottom of the Company's website (warrant@bitv.com) to request investigative assistance.

c) Warrants and requests for assistance received through the e-mail account will be acknowledged by the Company's Legal Team and responded to accordingly.

4.2.2 Victimized customers report to customer service agents

There are two scenarios when a customer experiences damage and wishes to file a complaint and report it:

a) Customers who have reported the case to law enforcement agencies: For customers who have reported the case to the police and other law enforcement agencies but still need the Company to take further measures, they can make inquiries or report the case to customer service agents.

b) Customers who have not reported the case to the law enforcement authorities: For customers who have not yet reported the case to the police and other law enforcement authorities but still need the Company to take measures, they can inquire or report the case to the customer service agents.

Even if a victimized customer inquires about or reports a case to customer service agents, in many cases, it is not possible to take immediate action due to the difficulty of identifying the member himself/herself. However, if a victimized customer's account is identified as having abnormal transactions in the "Abnormal Transaction Detection System," etc., the account may be frozen or the transfer of funds suspended, etc., regardless of the wishes of the member himself/herself.

4.3 Company Response

4.3.1 Search warrants and requests for assistance from law enforcement authorities

a) If a law enforcement agency sends a request for a search warrant execution or assistance, the Company provides a "Search Warrant Execution Inquiry" e-mail (warrant@bitv.com) at the bottom of its website to direct the issuance of a search warrant. It is important to include a copy of the law enforcement officer's license when sending this email. A search warrant from a law enforcement agency can result in the freezing of a customer's account.

b) The account of a customer who has received money from a victim of telecommunication and financial fraud can also be frozen if the victim has reported the case to the bank.

Note: The term "warrant execution inquiry" refers to a process by which a financial institution typically receives a search warrant from a law enforcement agency and executes it.

4.3.2 Response measures of customers who have reported to law enforcement agencies

a) Customer Service Team

i. Explaining to the customer that the response is limited due to the difficulty of confirming the exact content of the victimization, identification, etc., by filing a complaint by phone only.

ii. Customers are advised to change their passwords to ensure the security of their accounts.

iii. If the customer wishes to freeze or suspend the transfer of funds from the account, the following steps will be carried out:

In-person verification (name, date of birth, UID, cell phone number, email address)

Recording of customer statements requesting account freezing/suspension

Submission of applications for active freezing

iv. Executing measures such as account freezing/suspension of transfers, etc., pending approval from the Customer Service Team Leader.

v. Upon completion of measures such as account freezing/suspension of transfers, etc., the customer is notified of the relevant content (by phone, SMS, e-mail, etc.).

vi. Sharing relevant content via internal instant messenger. Recipients include:

Executive Group Members

The Customer Service Team Leader

The Security Team Leader

The Anti-Money Laundering Team Leader

The Legal Team

b) AML Team

i. The account is continuously monitored for unusual transactions.

ii. If unusual transactions are detected on the account, they will be reported and appropriate measures will be taken by the relevant procedures.

4.3.3 Response to customers who have not reported to the investigative body

a) Customer Service Team

i. Explaining to the customer that the response is limited due to the difficulty of confirming the exact content of the victimization, identification, etc., by filing a complaint by phone only.

ii. Customers are advised to immediately report the case to the police and other law enforcement agencies.

iii. Customers are advised to change their passwords to ensure the security of their accounts.

iv. If the customer himself wishes to freeze or suspend the transfer of funds from the account, the following steps will be carried out:

In-person verification (name, date of birth, UID, cell phone number, email address)

Recording of customer statements requesting account freezing/suspension

Submission of applications for active freezing

v. Executing measures such as account freezing or suspension of transfers, pending approval from the Customer Service Team Leader.

vi. Upon completion of measures such as account freezing/suspension of transfers, etc., the customer is notified of the relevant content (by phone, SMS, e-mail, etc.).

vii. Sharing relevant content via internal instant messenger. Recipients include:

Executive Group Members

Customer Service Team

Security Team

AML Team

Risk Management Department

Legal Team

b) AML Team

i. The account is continuously monitored for unusual transactions.

ii. If unusual transactions are detected on the account, they will be reported, and appropriate measures will be taken by the relevant procedures.

4.4 Procedures for refunding the amount of money victimized by telecommunication and financial fraud (telephone fraud)

4.4.1 Summary

The procedure for refunding the amount of money victimized by telecommunication and financial fraud is designed to refund amounts victimized that are not subject to the claim elimination procedure of the financial supervisory authority. The refund of victimized amounts is essentially based on an agreement between the fraudulent account nominee (member) and the victim of the

fraud.

4.4.2 Agreement situations between account holders (members) and victims

a) Customer Service Team

i. The Customer Service Team receives complaints related to the refund of the victimized amount, forwards the complaint to the relevant department via email, and then transfers the complaint to the Risk Management Department.

b) Finance Department

ii. Confirmation of the victim's cancellation of the application for victimization relief against the member's (account holder's) bank, cancellation of the claim elimination procedure, and confirmation of the lifting of the restriction on the payment of the victimized amount on the Company's bank account.

c) Risk Management Department

iii. The victim is directed to come to the Company along with the member (account holder) with their respective documents.

Victim

- Certificate (for victims)
- Identity cards
- Acknowledgement of facts signed by the victim
- Confirmation of accident facts
- Records of financial transactions (deposits and withdrawals)
- Copies of bank accounts

Members (account holders)

- Certificate
- Identity cards
- Acknowledgement of facts signed by the member
- Records of financial transactions (deposits and withdrawals)
- Copies of bank accounts
- Notification of claim elimination facts

iv. If the victim and the member (account holder) come to the Company with the required documents, the documents will be confirmed and the procedure of refunding the victimized amount will be carried out with the assistance of the Finance Department.

4.5 Failure to reach an agreement between the account holder (member) and the victim

4.5.1 Customer Service Team

The Customer Service Team receives complaints related to the refund of the victimized amount, forwards the complaint to the relevant department via email, and then transfers the complaint to the Risk Management Department.

4.5.2 Finance Department

Confirming that the Company's bank accounts have been frozen and share the results with the Customer Service Team, the Risk Management Department, and the Legal Team.

4.5.3 Risk Management Department

a) Informing the victim that the refund of the victimized amount is essentially based on an agreement between the account holder (member) of the telecommunication and financial fraud and the victim, and advising that the refund of the victimized amount may be difficult if the claim elimination process is in progress.

b) Persuading the victim to reach an agreement with the account holder (member) on the refund of the victimized amount.

c) Even if the victim and the account holder (member) fail to reach an agreement, in the event that the application for victimization relief is canceled to terminate the claim elimination procedure, the victim will be reminded of the possibility of refunding the victimized amount in the Company's bank account. In this case, the following documents will be required:

Self-declaration by account holders (members)	**Failure of account holders (members) to self-declare**
-Certificate (for victims) -Application for Cancellation of Victimization Relief -Confirmation of accident facts -Application for Complaints	-Certificate -Notification of termination of claim elimination -Confirmation of accident facts -Application for Complaints

d) Upon submission of the required documents by the victim, the documents will be confirmed and the process of refunding the victimized amount will be carried out with the assistance of the Finance Department.

e) If it is confirmed that the account holder (member) is involved in criminal facts, or if it is impossible to reach an agreement with the victim due to reasons such as the inability to locate him/her, and the victim files a lawsuit, the relevant content will be transferred to the Legal Team for a lawsuit response.

4.5.4 Legal Team

If subjected to a claim such as an action for the return of unlawful benefits, a litigation response will be commenced.

5. Wireline Complaint Response (Protecting Customer Service Personnel)

5.1 If the customer does not hang up without accepting the guidelines and persistent pestering:

Receiving and processing customer requests quickly, letting the customer realize that we are there to help them, and then informing them that we will verify the situation and get back to them within an appropriate time frame.

5.2 If a customer uses inappropriate language that includes swearing or sexual harassment:

We want to maintain respect on both sides while helping the customer deal with the problem. If a customer engages in continuous inappropriate swearing, we will warn the customer three times and may terminate the call if the problem continues.

5.3 If the customer asks for the call to be transferred to the highest responsible person or asks for contact information:

Due to organizational constraints, we are unable to provide contact information directly. We will report the content to our superiors and contact them in due course.

5.4 If a customer persists in using rude language or is a nuisance to our work:

We will create a blacklist within our Customer Service Team and immediately share the information within the team. If the issue is beyond the scope of the Customer Service Team, we will seek assistance from the relevant departments.

Schedules

Schedule 1:

***For claims for trading losses due to exchange vulnerabilities (and other claims), please use the same form**

BITV is a Hong Kong-based virtual asset exchange and ensuring the safety of our customers' assets is our top priority. If customers lose their assets due to unexpected problems, BITV will provide compensation if the loss is indeed caused by BITV's negligence after confirmation.

Customers are requested to provide the relevant information for the following items, and if all the information for each item has been submitted, we will conduct an internal review in turn. Please understand that the receipt result will be replied to by e-mail within two weeks, and may up to one month if there are unforeseen circumstances.

*Email to the address: verification-support@bitv.com
*Title of the email: "Compensation for the loss due to the restriction to deposit and withdrawal_UID"

[Customer's information]
Name, date of birth, cell phone number, UID, e-mail address
[Attached information]
The screenshot clearly shows the loss of money due to the vulnerability and an explanation of the situation.
(A detailed description including the date and time of the vulnerability, content of the vulnerability, tokens traded, markets traded, numbers of total buys/sells, token prices of total buys/sells, etc.)

BITV will always act in the position of the customer and appreciates your support. Thank you.

Schedule 2:

***Customers can claim compensation for any additional handling fees incurred as a result of not raising the withdrawal limit.**

BITV is a Hong Kong-based virtual asset exchange and ensuring the safety of our customers' assets is our top priority. If customers lose their assets due to unforeseen problems, BITV will provide compensation if the loss is indeed caused by BITV's negligence after confirmation.

Customers are requested to provide relevant information on the following items, and we will conduct an internal review in order if all the information on the items has been submitted. Please understand that the receipt result will be replied to by e-mail within two weeks, and may up to one month if there are unforeseen circumstances.

*Email to the address: verification-support@bitv.com
*Title of the email: "Compensation for loss due to deposit/withdrawal restriction_UID"

[Customer Information]
Name, Date of Birth, Cell Phone Number, UID, Email Address

[Attachment Information]
Your Authentication Information (contains screenshots of the results of each level of authentication)
Deposit and Withdrawal Limits (contains screenshots of the maximum limits for deposits and withdrawals)
Deposit and Withdrawal History (contains screenshots of all deposits and withdrawals made as a result of this issue and the fees charged)

BITV will always act in the position of the customer and appreciates your support. Thank you.