

October 24, 2026

Company Name:	GMO Internet, Inc.
Name of representative:	Tadashi Ito, President and CEO (Securities code: 4784; TSE Prime Market)
Inquiries:	Toshihiko Sugaya, Executive Officer (Telephone: +81-3-5728-7900)
Corporate website	https://internet.gmo/en

Notice Regarding Goodwill Payments to Customers and Compensation for Losses from Unauthorized Transactions Following Unauthorized Access

Regarding the unauthorized access by a third party to "Onamae.com Desktop Cloud" (hereinafter the "Service"), which is provided by GMO Internet, Inc. (hereinafter the "Company"), we hereby announce the following response policy, including goodwill payments to customers and compensation for losses from unauthorized transactions.

We deeply apologize for the considerable inconvenience and concern this matter has caused to our customers and all other parties concerned.

1. Overview

The Company has confirmed, through its investigation to date, that there is a security problem in the system of the Service, unauthorized access to the environment of the Service, and the fact that customers' information was taken outside. It has also received reports from some customers of transactions in their trading accounts that they do not recall making.

The Company, as an internet infrastructure provider that has been supported by many customers, takes this situation extremely seriously, and from the standpoint of giving top priority to the protection of customers, will take the following special measures.

2. Our Response Policy

(1) Goodwill Payment

The Company will make a goodwill payment of a uniform 5,000 yen to all customers who currently use the Service, regardless of whether they have suffered financial damage. This goodwill payment is made in respect of the inconvenience and anxiety this matter has caused to customers, and is separate from the compensation for losses from unauthorized transactions described in (3) below. The method of contacting eligible customers, the procedures for receiving the payment, and the payment timing will be announced by 23:59 on Friday, October 30, 2026, by email to registered email addresses.

(2) Provision of an Alternative Service and Six Months of Free Use

From the standpoint of giving top priority to customers' safety, the Company has decided not to resume the Service on its current system infrastructure, which was subject to the unauthorized access, and to fundamentally overhaul its security architecture. Accordingly, all customers who have a contract for the Service and wish to continue using a Windows desktop environment will be guided to migrate to an alternative service operated on an independent cloud infrastructure. After migration, the alternative service can be used free of charge for six months.

In providing the alternative service, the Company will confirm its safety, and will provide guidance before application so that customers can confirm the differences in functions and usage, precautions regarding migration, the scope of the free provision, and the fees and contract terms after the free period ends. The Company will not migrate customers to the alternative service without their consent. The start date of the provision, the application method, and the handling of contracts and usage fees for customers who do not wish to migrate will be announced by 23:59 on Friday, October 30, 2026, by email.

(3) Compensation for Losses from Unauthorized Transactions in Customers' Trading Accounts

If transactions not made by the customer's own will (hereinafter "unauthorized transactions") are carried out as a result of this unauthorized access, the Company will compensate for the realized losses incurred in the customer's trading account. The compensation covers realized losses (trading losses and fees, etc.) arising from transactions that the Company recognizes, as a result of its investigation, to be unauthorized transactions. Losses due to market fluctuations, profits that would have been earned from the transactions, and other indirect damages are not covered. The Company will determine eligibility based on transaction records, access records, and other materials, and may ask customers to submit additional materials. The Company will notify each customer individually of the result of its confirmation.

Where unauthorized transactions not made by the customer's own will have occurred, the Company asks customers (i) to submit information that allows the damage to be confirmed (information that allows the date, content, and amount of loss of the transactions in question to be objectively confirmed), and (ii) to explain to the relevant exchange, etc. the circumstances showing that the transactions resulted from unauthorized access by a third party, and to consult on the cancellation of the transactions and refunds, etc.

Details of the specific submission procedures for (i), including submission of identity verification documents and presentation of a dedicated password that allows the Company to directly check transaction history (view-only passwords for MT4/MT5 and others, etc. *1), will be announced separately.

If a refund is received from an exchange, etc., the Company will pay the remaining amount after deducting the refunded amount, and even if the exchange, etc. does not agree to a refund, the Company will pay the loss eligible for the compensation described above. If a customer receives compensation from the Company for the same loss despite having received a refund from an exchange, etc., or if an application is made that differs from the facts, the Company may ask the customer to return the amount.

The application method, required documents, application period, and payment timing will be announced by Friday, November 6, on the Company's official website and by email to registered email addresses. Customers' personal information and transaction information will be used only for the purpose of confirming this matter and providing compensation.

The Company will not ask customers for their passwords (excluding the passwords marked *1) or PIN numbers in connection with the compensation procedures. Please be cautious of any unfamiliar contact.

(4) Policy and Defensive Measures Regarding Malicious Threats from the Attacker

The Company has received a demand for money from a person believed to be the attacker in this matter. It has also been informed that, if the demand is not met, the attacker will take actions such as disclosing information about the Company and its customers. The details are as follows.

(i) Continuation of unauthorized manipulation (damaging account balances through unauthorized orders) of customers' trading accounts opened at more than 70 securities companies, FX companies, etc. in Japan and overseas

(ii) Unauthorized disclosure of information about the Service and the PCs of customers connected to the Service, and execution of a ransomware attack

(iii) Unauthorized disclosure of information about the Company's systems and operating structure

In response to such criminal acts targeting customers' important assets and information, the Company will respond as follows.

The Company will not comply with the attacker's demand, because even if the demand were met, there would be no guarantee that the acquired information would be deleted or that its unauthorized use would be prevented. It has consulted with the police and other relevant authorities regarding this matter and is responding in cooperation with them.

The Company has submitted all evidence, such as communication records, regarding the threats to the police (cybercrime division) and has requested a rigorous investigation as a criminal case. The attacker may disclose in the future what it claims to be information about the Company and its customers, and such information may include content that differs from the facts. Official announcements will be made through the Company's website, etc.; please be cautious of unreliable information.

As emergency defensive measures to protect customers' assets and information, the Company is taking the following measures as its highest priority.

Blocking of unauthorized transactions: It has requested and is coordinating with major exchanges and securities companies to block access via the Service, forcibly disconnect all active sessions, and urgently monitor and deter unauthorized transactions.

Blocking of communications: It has stopped network connections of the affected systems and blocked routes of unauthorized access from outside.

(5) Cooperation with Government and Investigative Authorities

The Company has made an initial report to the police and the competent authorities, and will continue to provide information to the relevant authorities and cooperate with the investigation. In light of the seriousness of this matter, and in order to prevent the spread of damage and the recurrence of similar attacks, it will also proceed with requests to the relevant government agencies, including the implementation of measures under Active Cyber Defense.

3. Impact on Our Consolidated Financial Results

The impact on our consolidated financial results of the goodwill payment and the compensation for losses, etc. cannot be calculated at this time. We will make an additional announcement as soon as the details become clear.

4. Chronology

The Company started an investigation on October 19, 2026, after receiving an inquiry from a customer, and on October 20 confirmed that an unauthorized program had been installed by a third party in the server environments of some customers of the Service.

On the same day, it suspended new applications and the control panel, and from 4:00 a.m. on October 21, it sequentially suspended the servers of all plans in order to prevent further damage.

Since October 21, the Company has received reports from customers of operations in their trading accounts that they do not recall performing, and has shared the situation with relevant business operators and requested their cooperation in implementing safety measures through guidance to customers. In addition, it consulted with the police on October 22.

The Company made announcements on October 21, 22, and 23, and announced the above response policy on October 24.

Proposal to the Government on Applying "Active Cyber Defense" to Protect the Nation's Assets

1. About Active Cyber Defense

Active Cyber Defense is a security framework in which, in response to serious threats in cyberspace, the government and relevant agencies take the lead in identifying and neutralizing (rendering harmless) attackers' infrastructure and intrusion routes before damage becomes severe, in order to prevent damage and prevent its spread. It goes beyond the conventional framework in which each business operator defends individually, and is positioned as an important national security measure for taking preemptive action against cyber attackers at the national level. For details of the government's discussions and related measures, please refer to the official materials of the Cabinet Secretariat

(Efforts on Cybersecurity: https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html).

2. Urgent Proposal to Relevant Government Agencies as the "First Activation Case"

This cyber attack goes beyond a mere system failure of a private service: an extremely malicious and

unprecedented method has been used, namely “unauthorized manipulation and destruction of assets targeting the trading accounts (financial assets) of ordinary citizens,” which goes beyond encryption and information theft. It is difficult for a private business operator alone, through defense and post-incident response alone, to eradicate the plundering of citizens’ assets by sophisticated cybercriminal groups operating across national borders.

Based on its social responsibility and sense of urgency as a business operator responsible for internet infrastructure, the Company has positioned this matter as the “first case of ‘activation’ of Active Cyber Defense to protect the property of the people and trust in cyberspace,” and has strongly submitted a proposal (urgent request) to the relevant government agencies to take effective measures aimed at tracing, blocking, and neutralizing the attack infrastructure under national leadership. It will continue to spare no effort in providing all logs and breach information to the government and investigative authorities, and will do its utmost to eradicate cybercrime in cooperation with the government.

5. Future Information Disclosure and Contact for Inquiries

The Company plans to announce further information on its website and elsewhere as it becomes available, and will also promptly announce any newly disclosable facts.

Contact for inquiries regarding the Service:

Inquiry form: <https://help.onamae.com/contact/>

Telephone: +81 3 5456 2560 (24 hours, including weekends and holidays)

(Reference) Previously Announced Materials

- Announced on October 21, 2026 (as of 4:00 a.m.): <https://internet.gmo/en/news/article/246/>
- Announced on October 22, 2026 (as of 4:59 p.m.): <https://internet.gmo/en/news/article/247/>
- Announced on October 23, 2026 (as of 4:10 p.m.; Japanese only): <https://internet.gmo/news/article/248/>
- Announced on October 24, 2026 (as of 11:50 a.m.; Japanese only): <https://internet.gmo/news/article/249/>