Press Release:

Note: This document has been translated from the Japanese original for reference purposes o nly. In the event of any discrepancy between this translated document and the Japanese orig inal, the original shall prevail.

November 10, 2026

Company name:	EDION Corporation
Job title and name of representative:	Masataka Kubo, Representative Director, Chairman and CEO
Securities Code:	2730 (TSE Prime Market)
Inquiries:	Tsugunori Ishida, Director, Managing Executive Officer and Chief Corporate Planning Officer

Notice Regarding the Leakage of Personal Information and Suspension of Services Due to Unauthorized Access to the EDION E-Commerce Site

On November 6, 2026, EDION Corporation (the "Company") published a notice on its corporate website regarding the potential leakage of personal information due to unauthorized access to the EDION E-Commerce (EC) site (hereinafter "the EC site"). However, through subsequent monitoring and detailed investigation, new facts concerning the initial incident have come to light, and traces of unauthorized access utilizing a new attack method have been confirmed.

In response, prioritizing the prevention of further damage, we implemented an emergency suspension of various services, including the EC site, effective 10:00 p.m. on Saturday, November 7, as a preventive measure. We hereby report the current status and our countermeasures, combining the overview of the first report with the newly identified events (the second report).

We sincerely and deeply apologize for the significant inconvenience and concern this has caused our customers and all related parties.

1. Chronology of the Incident and Emergency Suspension of Services

(1) Overview of the First Report (Announced November 6, 2026)

On November 6, 2026, we announced that unauthorized external access exploiting a system vulnerability occurred at approximately 6:30 p.m. on Thursday, November 5, 2026, against a portion of the server area storing 'log files' (which temporarily record the communication processing of the EC site), resulting in the potential leakage of personal information, including names, addresses, and phone numbers of up to 13,685 customers.

(2) Overview of the Second Report (Announced Nov. 9, 2026 on the Corporate Website)
As a result of our continuous investigation, in addition to new information leakages related to the unauthorized access disclosed in the first report, we newly discovered that a malicious program had been injected into the payment processing section of the EC site by an external third party.

To prevent the expansion of damages, we implemented an emergency suspension of related services at 10:00 p.m. on Saturday, November 7.

2. Scope of Identified and Potential Information Leakage (Under Investigation)
As details regarding the events of the second report outlined in "1. (2)" above, the leakage of information and the potential thereof have been confirmed with respect to the following two matters:
(1) Findings from Further Investigation Regarding the First Report (Correction to the First Report)
As a result of the investigation into the incident reported in the first announcement, it was newly confirmed that the affected information also included the following:

- Credit Card Information (Order error logs: Up to 5 records)
  Affected information: Credit card number, expiration date, cardholder name, and security code.
  *Note: This applies strictly to exceptional cases where input data was temporarily recorded in the system log when an error occurred on the order screen.
- EDION Gift Card Information (5,360 cards)
  Information compromised: Gift card number, PIN, and usage history. *Note: The only environment where these cards can be used solely by entering the card number and PIN is the EC site. Because usage at physical stores requires the presentation of the actual physical card, and the EC site is currently suspended, it is structurally impossible for a third party to fraudulently use the leaked information at this time.
- Login IDs and Passwords (Up to 1,141 users)
  *Note: As the EC site requires two-factor authentication (2FA) for new logins, the situation does not allow for immediate unauthorized use. However, to ensure absolute security, we will individually email affected customers requesting them to change their passwords.

(2) Impact of the Newly Identified Malicious Program
It has been confirmed that the newly identified malicious program had been active starting shortly after 7:00 p.m. on Wednesday, November 4.
While credit card payment processing on the EC site complies with "non-retention" standards and does not store card information on servers, this incident involved a malicious program that had been injected into the payment information entry process for personal computer (PC) environments. Consequently, we cannot rule out the possibility that personal information, including credit card information entered on the payment screen via PCs during the period in question, was intercepted and directly leaked to an external third party.

Affected information: Credit card number, expiration date, cardholder name, and security code

Number of affected transactions: Up to 556 (in cases where credit card information was newly entered on the payment information entry screen)

*Note: It has been confirmed that operations and payment entries made via smartphones were not subject to the malicious program in question.

3. Coordination with Credit Card Companies and Measures to Prevent Gift Card Fraud

(1) Response Regarding Credit Cards

To prevent fraudulent use, we have formally requested our affiliated credit card companies to enhance their monitoring for the up to 5 cards recorded in the order error logs and the up to 556 cards newly entered by customers using a PC environment during the affected period (after 7:00 p.m., Nov. 4). We will continue to work closely with the card companies on this matter.

(2) Response Regarding EDION Gift Cards

As stated above, because the EC site is currently suspended, the 5,360 compromised EDION Gift Cards cannot be fraudulently used by third parties using only the leaked data. We are currently reviewing how to handle these cards moving forward to ensure customer peace of mind. We will notify affected customers as soon as our policy is finalized.

4. Operational Status of Services

To contain the damage, we suspended the EC site, the "EDION Official App," and the "EDION Smart App" at 10:00 p.m. on Saturday, November 7. The current status is as follows:

(1) The EC Site (Currently suspended / Reopening date TBD)

The service remains suspended.

(2) EDION Official App and EDION Smart App (Partial functions resumed)

After conducting a comprehensive inspection of linked server environments and files, we confirmed that they were not affected by the malicious program. Having ensured sufficient safety, we resumed limited services such as the "Digital Membership Card" and "Coupon Display" functions at 9:10 p.m. on Sunday, November 8.

5. Requests to Customers

・Review of Credit Card Statements:

For customers who entered new credit card information on the EC site via a PC during the affected period (after 7:00 p.m., Nov. 4), we sincerely request that you review your credit card statements for any unrecognized charges. Should you notice any suspicious charges, please contact the inquiry desk listed on the back of your card. We have also requested affiliated credit card companies to strengthen monitoring against fraudulent usage during the period in question.

・Password Reset Request (Individual contact to affected customers):

We will individually contact the 1,141 affected customers by email to request a password change. We apologize for the inconvenience, but we kindly ask customers who receive this

email to change their passwords in accordance with the instructions provided.

・Caution Regarding Suspicious Communications:

Please remain vigilant against suspicious emails, SMS messages, or phone calls pretending to be from the Company.

6. Future Actions

Regarding this matter, we are currently preparing to submit follow-up reports to the Personal Information Protection Commission (PPC) and the police department having jurisdiction. We will promptly make an announcement as soon as any new facts come to light, such as the identification of the scope of impact.

7. Impact on Financial Results

The impact of this matter on the Company's consolidated financial results is immaterial. If any matters requiring disclosure arise in the future, we will promptly make an announcement.