This document has been translated from the Japanese original for reference purposes only.
In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail. The Company assumes no responsibility for this translation or for direct, indirect or any other forms of damages arising from the translation.

January 6th, 2025

Company name: Modalis Therapeutics Corporation
Stock exchange listing: Tokyo Stock Exchange
Code number: 4883
URL: https://www.modalistx.com/en/
Representative: Haruhiko Morita

Notice Regarding the Occurrence of an Incident of Electronic Fraud at a Subsidiary and the Recording of an Extraordinary Loss

30-Dec-2024 TOKYO & Waltham, Mass – Modalis Therapeutics Corporation (Tokyo Stock Exchange: 4883), a pioneering company developing innovative products for the treatment of rare genetic diseases utilizing its proprietary CRISPR-GNDM® epigenome editing technology, regrets to inform you that a special loss has occurred due to an electronic fraud incident at its U.S. subsidiary. This incident occurred due to fraudulent payment instructions by a third party posing as a business partner and resulted in a loss of 90,000 USD. We would like to express our sincere apologies to our shareholders and other stakeholders for any inconvenience or concern caused by this incident.

1. Overview of the Incident

At the beginning of 2023, our subsidiary engaged a company (hereinafter referred to as "Contractor") for tasks, with the deliverables completed in late August as agreed. In the end of November, a person impersonating Contractor (hereinafter referred to as the "Perpetrator") sent an email requesting payment for the tasks. Our subsidiary inadvertently processed this payment to the Perpetrator's fraudulent bank account.

2. Background of the Incident

Contractor is a manufacturing contractor with a U.S. base. We had multiple prior transactions with Contractor, which consistently met delivery and quality standards and responded flexibly to changes in orders or specifications. However, during one such transaction, the Perpetrator somehow gained access to the official email account of Contractor’s representative. Using this access, the Perpetrator sent an invoice related to a legitimate transaction from legitimate Contractor’s email server. Following the instructions in the email, our subsidiary's finance team transferred the payment to the fraudulent account.

3. Subsequent Developments

The fraud came to light when Contractor's finance department sent a follow-up payment request for the same transaction. Upon investigation, we discovered that the initial payment had been made to a fraudulent account. We immediately contacted local authorities, our bank, and the Perpetrator's bank, successfully freezing the fraudulent account. As the results, we were able to confirm most of the transferred funds remained in the Perpetrator's account. Following months of negotiations and procedures with both banks, significant amount of the funds was recovered. After discussions with Contractor, we agreed to share the financial burden of the remaining loss proportionally. Additionally, we filed an insurance claim for electronic fraud and received partial compensation. Ultimately, our net loss was concluded at 90,000 USD.

4. Known Facts at This Stage

Law enforcement has been investigating the incident since the fraud was discovered, but no significant leads on the Perpetrator have been found. Through our legal representatives, we sought additional information from the banks involved, but further details could not be obtained due to confidentiality restrictions. The sophistication of the emails, including accurate timing and content, suggests the Perpetrator monitored communications between our company and Contractor over time. This indicates a highly calculated and advanced method of fraud.

5. Potential Personal Information Leak

Our investigation confirmed no leak of customer information held by our company. To date, there is no evidence to suggest personal information has been compromised.

6. Measures to Prevent Recurrence

While the breach originated from Contractor's email account, we will implement stricter password protection and two-factor authentication for our email and communication tools. We will also establish additional verification procedures, such as using multiple communication methods to confirm payment instructions. Internally, we are reviewing and strengthening our payment processes. Additionally, we are working closely with our banks to stay updated on the latest fraud prevention measures. Fraudulent approaches targeting our company, though unsuccessful in other cases, are frequent, and we are committed to enhancing our risk management framework.

7. Impact on Financial Performance

This incident resulted in a special loss of 90,000 USD (approximately 14 million JPY), which will be reflected in our 2024 4th quater financial results. While the majority of the misappropriated funds were recovered, we sincerely apologize for the financial damage caused to our shareholders and investors.

We will continue to work diligently to ensure such incidents do not recur.

About Modalis:

Modalis Therapeutics develops precision genetic medicines using epigenome editing technology. Modalis is pursuing therapies for orphan genetic diseases using its proprietary CRISPR-GNDM® technology which enables the gene/locus-specific modulation of gene expression or epigenetic editing without the need for DNA cleavage or altering DNA sequence. Headquartered in Tokyo with laboratories and facilities in Waltham Massachusetts, the company is listed on Tokyo Stock Exchange's Growth market. For additional information, visit www.modalistx.com.