December 10, 2021

Dear valued customers,

It is regret to inform you that we received some reports about our email has been used as spoofing mails.

1. Summary of the fact:

In August 2020, the malware called “EMOTET” has invaded our server and started to send targeted e-mail.

This malware is characterised as below:

1) Steal all histories of sender’s outbox

2) Send spoofing mail using stolen address randomly

Though the “EMOTET” was disrupted through global action in January 2021,

once this unauthorised access was established,

these were sold to other top-level criminal groups to deploy further illicit activities,

such as data theft and extortion through ransomware.

2. What we had done after August 2020:

1) We have renewed our server to protect with stronger security

2) We have updated with stronger cybersecurity system

3) We have strengthen the Firewall

3. How to deal with spoofing mails when you find:

Please be the most cautious NOT to open and download the attachment,

and/or click on a malicious link in the spoofing mails.

When you receive spoof mails, check with preview first and delete them immediately.

For your reference, attachments could be: MS Word, Excel, Memo pad and so on. Finally,

it is highly recommended to updated cybersecurity software regularly.

We apologize for causing you inconvenience

Riken Perfumery Co., Ltd.