Notice regarding the unauthorized access to Shalom, the system used by LINE's subcontractor

2023.07.11

To former employees of LINE,

We have been notified by our labor and social security attorney's office, where we outsource the handling of application for social and labor insurances, that there was a ransomware attack on June 9 against the data server of MKSystem Corporation, which is the vendor for operating Shalom (hereinafter "the System") used by the office. According to the notification, the possibility of information leakage cannot be denied.

Occurrence and response (Japan Time)

- June 5, 2023, around 6:00 am: MKSystem Corporation's server went down.

- Investigation discovered a possibility of unauthorized access, and an immediate action was taken to disconnect the relevant internet connections.

- MKSystem Corporation continued investigation and confirmed an unauthorized access with ransomware by a third party. Within the same day, they established a task force and reported to the Cybersecurity Division of Advanced Information Promotion Bureau of the Osaka Prefectural Police.

- June 6, 2023: MKSystem Corporation announced the ransomware infection caused by a third-party attacker.

- June 8, 2023: In response to the possibility of information leakage, MKSystem Corporation reported to the Personal Information Protection Commission.

Although there is no evidence found at the moment (as of July 5, 2023)—according to MKSystem Corporation—that personal information has been sent externally or abused, we take this incident very seriously and believe it is important that you are properly informed as former LINE employees. (Please note that the Social Security and Tax Number, i.e. My Number, and email address are not stored in the System.)

We will notify you separately in the case that new information is discovered, including when we find evidence of information leak, etc. Meanwhile, we fully comply with the requirement to report to the competent authority.

1. Data with a potential danger of information leak

As we have used the System only for the following procedures, there is a potential risk of data breach with the items mentioned below.

Applications for childcare/nursing care leave allowance.

Name on family registry with ruby characters (if an applicant submit a form to register a name change when applying for the benefits, former and current name can be included), address, phone number, gender, date of birth, employment insurance number, bank account details, monthly salary, spouse's employment insurance number(only those who applied for "Mom & dad child care leave"), childcare/nursing care leave related data. (such as number of days)

Applications to register a change of address (by the end of March, 2018)

Name on family registry with ruby characters, address, the basic pension number, spouse's name on family registry with ruby characters, date of birth (married couple only)

Applications to register a name change (by the end of March, 2018)

Former and current name on family registry with ruby characters, date of birth, the basic pension number, employment insurance number.

Applications to register acquisition or loss of employment insurance qualification (by the end of 2017)

Name on family registry with ruby characters (if an applicant submit a form to register a name change when applying for the benefits, former and current name can be included), address, phone number, gender, date of birth, date of acquisition or loss of employment insurance qualification, employment insurance number, monthly salary, reason for resignation, residence card data.

Applications to claim for industrial accident compensation insurance

Name on family registry with ruby characters, address, phone number, gender, date of birth, bank account details, monthly salary, incentives, details of industrial accidents (e.g. causes of accidents, symptoms, medical facilities, pharmacies etc.)

2. Response going forward

We are conducting a fact-check through the labor and social security attorney's office that we delegate the tasks to specify what personal information is involved and whether there is a data breach. We will consider how to improve security measures in our system including outsourcing entities.

3. Potential risks of secondary damage

Although the investigation has not been completed yet, as of now, it shows no evidence for information leak and/or secondary damage caused by data misuse, etc. Should any secondary damage be identified, we will certainly provide necessary information. We take the protection and the proper use of your data very seriously, please be advised to remain vigilant against suspicious contacts and activities. We sincerely apologize for the inconvenience this may cause.

4. Inquiries regarding this incident

Contact payroll team: dl_jinji_payroll_02@linecorp.com