January 12, 2021

3-1-3, Uchihiranomachi, Chuo-ku, Osaka
Capcom Co., Ltd.
Haruhiro Tsujimoto, President and COO
(Code No. 9697 First Section of Tokyo Stock Exchange)

3rd Update Regarding Data Security Incident Due to Unauthorized Access

Capcom Co., Ltd. (Capcom) has previously confirmed that it has been the victim of a customized ransomware attack following unauthorized access to its network and has verified that some personal information maintained by the Capcom Group has been compromised.

On November 16, 2020 (JST) Capcom announced that it had verified that the personal information of 9 people had been compromised in this attack. As an update to its ongoing investigation, the company has verified that the personal information of an additional 16,406 people has been compromised, making the cumulative number since this investigation began 16,415 people. Further, the company has also ascertained that the potential maximum number of customers, business partners and other external parties etc., whose personal information may have been compromised in the attack is approximately 390,000 people (an increase of approximately 40,000 people from the previous report), the details of which are listed in "2. Potentially compromised data (updated)" below.

Capcom offers its sincerest apologies for any complications and concerns that this may bring to its potentially impacted customers as well as to its many stakeholders.

As there is an ongoing investigation in place, it is possible that new facts may come to light going forward. Below is a general summary of what new information has been confirmed at this point in time (as of January 12, 2021). Further, because the overall number of potentially compromised data cannot specifically be ascertained due to issues including some logs having been lost as a result of the attack, Capcom has listed the maximum number of items it has determined to potentially have been affected at the present time.

1. Information verified to have been compromised (updated)

i. Personal Information	16,406 people *cumulative total since investigation began: 16,415 people ・Business partners, etc.: 3,248 people At least one of the following: name, address, phone number, email address, etc. ・Former employees and related parties: 9,164 people At least one of the following: name, email address, HR information, etc. ・Employees and related parties: 3,994 people At least one of the following: name, email address, HR information, etc.
ii. Other Information	Sales reports, financial information, game development documents, other information related to business partners

2. Potentially compromised data (updated)

i. Personal Information	Applicants: approx. 58,000 people At least one of the following: name, address, phone number, email address, etc. *Cumulative maximum number of potentially compromised data for customers, business partners and other external parties: 390,000 people *Regarding the cumulative maximum number of potentially compromised data above: as part of its ongoing investigation, Capcom has determined that it currently does not see evidence for the possibility of data compromise for the approximate 18,000 items of personal information from North America (Capcom Store member information and esports operations website members) that the company included in its November 16, 2020 announcement. As such, these have been removed from this cumulative maximum number of potentially compromised data.

None of the at-risk data contains credit card information. All online transactions etc. are handled by a third-party service provider, and as such Capcom does not maintain any such information internally.

Additionally, the areas that were impacted in this attack are unrelated to those systems used when connecting to the internet to play or purchase the company's games online, which have continued to utilize either an external third-party server or an external server. As such, these systems have been unaffected by this ransomware attack and it is safe for Capcom customers or others to connect to the internet to play or purchase the company's games online.

3. Support for individuals whose personal information or corporate information has been confirmed to have been compromised and those whose information has potentially been compromised
   i. Action addressing personal or corporate information confirmed to have been compromised
   Capcom is contacting individuals whose information it has verified to have been compromised to discuss the background of this incident and current situation.

   ii. Action addressing potentially compromised personal information
   Capcom is continuing the investigation into information that has potentially been taken or compromised. For individuals who wish to inquire about personal information that has potentially been compromised, please contact the following support desks in your country or region:

   Japan: Capcom Data Security Incident Support Line (Japanese only)
   Tel. (toll-free): Game customer inquiries 0120-400161
   General inquiries 0120-896680
   Hours: 10:00 AM – 8:00 PM

   North America: Capcom USA Customer Support Page
   www.capcom.com/support

   EMEA: Capcom Europe Customer Support
   feedback@capcom.com

4. Measures going forward
   i. Capcom will continue coordinating with law enforcement authorities in Japan and the U.S., and also give timely reports to and receive advice from the institutions responsible for the protection of personal information in each country.
   ii. The company is working with parties such as a major IT security specialist company to work toward understanding the overall damage caused by the attack and preventing any reoccurrence. A report will be issued following the close of the investigation.
   iii. Capcom is continuing to work toward improving its security going forward, with activities that include holding preparatory meetings ahead of the launch of its Information Technology Security Oversight

Committee, which will function as an advisory group on matters related to system security from external security experts. Two university professors, one external lawyer and one certified public accountant that is an IT system audit specialist, all of whom possess extensive knowledge in the field of security, have agreed to join this committee.

At this point in time, Capcom's internal systems have in large part recovered, and business operations have returned to normal. Further, while there have been no changes to the forecast for the Capcom Group's consolidated business results (for the fiscal year ending March 31, 2021), the company will swiftly make an announcement in the case that any further disclosure is necessary.

Capcom would once again like to reiterate its deepest apologies for any complications or concerns caused by this incident. As a company that handles digital content, it is regarding this incident with the utmost seriousness. In order to prevent the reoccurrence of such an event, it will endeavor to further strengthen its management structure while pursing legal options regarding criminal acts such as unauthorized access of its networks.

Inquiries regarding the above information may be directed to:

Press Contact
North & South America: https://press.capcom.com
Europe, Middle East & Africa: https://www.capcomeuro-press.com

Customer Support
North & South America: www.capcom.com/support
Europe, Middle East & Africa: feedback@capcom.com

Investors
Public Relations and Investor Relations Section
(Tel)+81-6-6920-3623 (Fax) +81-6-6920-5108

Business Partners
Please contact the representative department with which you work