

NOTICE OF DATA SECURITY INCIDENT

DataLogic Software, Inc. (“DataLogic”) recently experienced a security incident that may have impacted the protected health information (“PHI”) of 7,200 individuals whose information was provided to DataLogic for processing on behalf of the Texas Health and Human Services Commission (“TX HHSC”). DataLogic provides Medicaid Electronic Visit Verification and claims processing services for TX HHSC and has informed them of the security incident.

What happened?

On December 5, 2020, DataLogic discovered a security incident impacting certain systems. As soon as we learned of the incident, we began an internal investigation and took the impacted systems offline to address the incident and ensure the security of our environment. We also began working with independent cybersecurity specialists to help us determine what had occurred, and whether any information was at risk. The investigation determined that on November 30, 2020, an unauthorized actor gained access to certain DataLogic systems and, on December 5, 2020, deployed malware within the environment. The investigation also showed that our application databases were not accessed, and information stored in these databases remains secure. However, the investigation determined that certain files containing PHI may have been accessed by the unauthorized actor. DataLogic worked with cybersecurity specialists to perform a detailed review of the files, and on January 19, 2021, identified those individuals whose PHI was impacted by the incident. Letters were mailed to impacted individuals and appropriate regulatory agencies on February 3, 2021.

What information was involved?

From our investigation, it appears that impacted information may have included member names, addresses, dates of birth, state Medicaid numbers, and health and treatment-related information. For 188 individuals, Social Security numbers were also impacted.

What is DataLogic doing?

DataLogic is offering individuals whose Social Security numbers were impacted credit monitoring and identity theft protection through IDX at no cost. DataLogic has also taken steps to minimize the risk of a similar event from happening in the future, including resetting all passwords and implementing additional controls for all types of remote access to its systems. In addition, we have notified and are cooperating with federal law enforcement.

For more information: To determine whether your information was impacted or for more information about this incident, please call 1-833-726-0932 Monday through Friday from 8 am - 8 pm Central Time. Individuals can also contact the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 or visit www.ftc.gov/idtheft/ for more information on protecting their identity.

AVISO DE INCIDENTE DE SEGURIDAD DE DATOS

DataLogic Software, Inc. (“DataLogic”) recientemente experimentó un incidente de seguridad que pudo haber afectado la información médica protegida (“*PHI*”, por sus siglas en inglés) de 7,200 personas cuya información fue proporcionada a DataLogic para procesarse en nombre de la Comisión de Salud y Servicios Humanos de Texas (“*TX HHSC*”, por sus siglas en inglés). DataLogic proporciona Verificación electrónica de visitas de Medicaid y servicios de procesamiento de reclamos para la *TX HHSC* y les ha informado del incidente de seguridad.

¿Qué sucedió?

El día 5 de diciembre de 2020, DataLogic descubrió un incidente de seguridad que afectó ciertos sistemas. En cuanto nos enteramos del incidente, comenzamos una investigación interna y desconectamos los sistemas afectados para abordar el incidente y garantizar la seguridad de nuestro entorno. Empezamos también a trabajar con especialistas en ciberseguridad independientes para ayudarnos a determinar lo que había ocurrido y si alguna información estaba en riesgo. La investigación determinó que el día 30 de noviembre de 2020, un actor no autorizado obtuvo acceso a ciertos sistemas de DataLogic y, el día 5 de diciembre de 2020, desplegó malware dentro del entorno. La investigación mostró también que el actor no autorizado no accedió a nuestras bases de datos de aplicaciones y que la información almacenada en dichas bases de datos permanece segura. No obstante, la investigación determinó que ciertos archivos que contenían *PHI* pudieron haber sido accedidos por el actor no autorizado. DataLogic trabajó con especialistas en ciberseguridad para realizar una revisión detallada de los archivos y, el día 19 de enero de 2021, identificamos a aquellas personas cuya *PHI* se vio afectada por el incidente. El día 3 de febrero de 2021, se enviaron cartas a las personas afectadas y a las agencias reguladoras apropiadas.

¿Qué información se vio afectada?

De nuestra investigación se desprende que la información afectada pudo haber incluido nombres, domicilios, fechas de nacimiento, números de Medicaid estatales e información relacionada con la salud y tratamiento de los miembros. Los números de Seguro Social de 188 personas se vieron también afectados.

¿Qué está haciendo DataLogic?

DataLogic está ofreciendo, sin costo alguno, monitoreo de crédito y protección contra el robo de identidad a través de *IDX* a las personas cuyos números de Seguro Social se vieron afectados. DataLogic ha tomado también medidas, incluyendo el restablecimiento global de contraseñas y la implementación de controles adicionales para todo tipo de acceso remoto a sus sistemas, para minimizar el riesgo de que esto suceda en el futuro. Además, hemos notificado y estamos cooperando con agencias federales del cumplimiento de la ley.

Para mayor información: Para determinar si su información se vio afectada o para mayor información sobre este incidente, sírvase llamar al 1-833-726-0932 lunes a viernes de 8 a.m. a 8 p.m. hora Central. Las personas pueden también comunicarse con la Comisión Federal de Comercio a Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC. 20580, 1-877-ID-THEFT (1-877-438-4338); TTY (teléfono de texto): 1-866-653-4261 o visitar www.ftc.gov/idtheft/ para más información sobre cómo proteger su identidad.