



**FOR IMMEDIATE RELEASE:**

May 12, 2023

**FOR MORE INFORMATION:**

HFS: [Jamie.Munks@illinois.gov](mailto:Jamie.Munks@illinois.gov)

IDHS: [Marisa.Kollias@illinois.gov](mailto:Marisa.Kollias@illinois.gov)

**Notice to the Media  
Incident Involving Protected Health Information**

**SPRINGFIELD** – Pursuant to the requirements of the Health Insurance Portability and Accountability Act, 45 CFR Sections 164.400-414, and the Illinois Personal Information Protection Act, 815 ILCS 530/12, the Illinois Department of Healthcare and Family Services (HFS) and the Illinois Department of Human Services (IDHS) (collectively, the Departments) are notifying the media of an incident within the State of Illinois Application for Benefits Eligibility (ABE) system’s Manage My Case (MMC) portal.

The ABE system is the eligibility system for State-funded medical benefits programs (Medicaid), the Supplemental Nutrition Assistance Program (SNAP), and Temporary Assistance for Needy Families (TANF). The MMC portal within ABE enables Departments’ customers to see their case history and benefit details, as well as change account and benefit information. On March 13, 2023, the Departments discovered suspicious user accounts had been created within the ABE system. These suspicious accounts were able to link to existing customer MMC accounts by providing the customer’s date of birth and Individual ID or Social Security Number, and then correctly answering several identity proofing questions. The Departments believe customer personal information had been stolen elsewhere - through no fault of the Departments - and this stolen personal information was then used to access customer MMC accounts. The information that could have been viewed within the MMC portal includes the client’s name, address, phone number, date of birth, recipient identification number, individual ID, Case ID, Social Security Number, benefits applied for and received, and income information. If the client applied for benefits through the ABE portal, the application and any documents uploaded to support the application could be viewed. Information of individuals included on the application for benefits or receiving benefits with the household could also have been viewed.

In response to this incident, the Departments deployed a new software to stop the creation of more suspicious user accounts and de-linked the suspicious accounts from the customer accounts.

The Departments notified the potentially affected individuals, the members of the Illinois General Assembly and the Office of the Illinois Attorney General on May 12, 2023.

The Departments are providing a dedicated phone line to provide assistance and answer customer questions about this incident. Individuals with a question about this incident can call 1-877-657-0006. The assistance line is available until August 14, 2023. Potentially affected individuals can also contact consumer reporting agencies to place a free fraud alert or security freeze on their accounts, or the

Federal Trade Commission to learn more about fraud alerts, credit freezes, or other identity theft resources.

Contact information for consumer reporting agencies:

- Equifax
  - [www.equifax.com/personal/](http://www.equifax.com/personal/)
  - P.O. Box 105788, Atlanta, GA 30349
  - 1-800-525-6285 (fraud alert)
  - 1-888-298-0045 (credit freeze)
- Experian
  - [www.experian.com](http://www.experian.com)
  - P.O. Box 9554, Allen, TX 75013
  - 1-888-397-3742 (fraud alert)
  - 1-888-397-3742 (credit freeze)
- TransUnion
  - [www.transunion.com](http://www.transunion.com)
  - P.O. Box 2000, Chester, PA 19016
  - 1-800-680-7289 (fraud alert)
  - 1-888-909-8872 (credit freeze)

Contact information for the Federal Trade Commission:

- [www.ftc.gov](http://www.ftc.gov)
- [Identity Theft Recovery Steps | IdentityTheft.gov](http://IdentityTheftRecoverySteps.IdentityTheft.gov)
- Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, D.C.20580, 1-877-382-4357 (Consumer Help Line)