**Commonwealth of Kentucky**
**Personnel Cabinet**

**Andy Beshear, Governor** **Gerina Whethers, Secretary**

**FOR IMMEDIATE RELEASE**

**Contact: Russell Goodwin**
502-564-6791
Russell.Goodwin@ky.gov

# StayWell Provides Increased Security Controls in Response to Incident

## KEHP members encouraged to follow Consumer Reports best practices

**FRANKFORT, Ky. (June 3, 2020) –** On April 27, the Kentucky Personnel Cabinet was notified of a security incident involving the well-being and incentive program portal hosted by StayWell at KEHPLivingWell.com. StayWell is a third-party vendor that administers the well-being program on behalf of the Kentucky Employees' Health Plan (KEHP).

The security incident was related to a malicious attack against StayWell's portal, which occurred in two rounds: an initial round taking place from April 21–27 and a secondary round taking place from May 12-22.

After thorough investigation of the incident, StayWell determined that the attack was likely associated with a bad actor who had access to a set of valid KEHP member email addresses and passwords from a previous unidentified data leak in a non-StayWell system.

As a result of the investigation, StayWell determined that a security breach had occurred in that the attacker used the valid KEHP member logins to access 971

member accounts on its platform, with a small subset of these members also having had their Commonwealth email accounts accessed. The nature of the attack resulted in fraudulent gift card redemptions and exposed biometric screening and health assessment data.

Members' financial data or personal information, i.e., Social Security numbers, date of birth, or addresses, were not compromised in the incident. The scope of the first round of the attack was isolated to StayWell's portal. The scope of the second round of the attack involved a small subset of KEHP members, targeting potential victims who likely used the same password across multiple systems, accounts, and programs. The Commonwealth has no reason to believe that the Commonwealth's human resources systems or data were affected at any point during either round of the attack.

Immediately upon becoming aware of the first round of the attack, StayWell temporarily disabled the KEHP LivingWell site to review site security measures and prevent any further unauthorized access or disclosure of participant data. StayWell also implemented additional user controls to ensure added security for members. Communications regarding the security incident were distributed to all affected members.

StayWell is in the process of restoring all 971 member accounts, including affected member incentive accounts, to pre-incident status.

The Commonwealth Office of Technology, the Personnel Cabinet, and StayWell take data incidents like this very seriously and encourage KEHP members to use "strong passwords" and other best practices outlined by Consumer Reports. Members should always refrain from using the same password for multiple systems, accounts, and programs.

For questions related to this incident, members can contact StayWell at 1-866-746-1316 or KEHPLivingWell@staywell.com. Pursuant to KRS 61.931 et. seq., the Personnel Cabinet has notified the Kentucky Attorney General's Office, the

Auditor of Public Accounts, the Kentucky State Police, and other state agencies of this security incident.

###