

TO: Chief Operation Officers – Regent Institutions

FROM: Kansas Information Security Office (KISO)

DATE: June 5, 2020

RE: Unemployment Insurance (UI) Fraud

What is Happening: The Kansas Department of Labor has received multiple reports from employees associated with all levels of government, (healthcare, education, higher education, and first responders) indicating that they received a notice of filing an unemployment claim, when they had not. In many cases, employees in these areas have not suffered from furloughs or layoffs. Malicious actors are exploiting these individuals' information because they know that they are less likely to collide with legitimate unemployment claims by filing against people in these sectors.

There have been multiple reports from various states and the federal government that indicate the malicious actors are likely using individuals' information obtained from previous private sector breaches. The bad actors then hang onto the information to use it in times like now. In late May, MS-ISAC reported similar issues in at least 12 states. They also believe most of the data being exploited to be slightly dated. In addition, it is believed that the malicious actors are then matching that information with public databases on public employees to target their fraudulent unemployment insurance filings. By targeting these individuals, they increase their chances of slipping through and receiving a fraudulent pay out.

What is Being Done by KDOL: The Kansas Department of Labor is aware public sector, higher education, education, and first responders are being targeted. KDOL staff are taking steps to try and validate the incoming claims against additional data that they have on file to ensure only valid claims are processed. They are also attempting to identify any potential identity theft. The KISO is actively engaged in monitoring and preventing cyber threats that have arisen out of the current COVID-19 pandemic situation.

What Identity Theft Victims Should Do: If you have employees that have not been furloughed, and report that an unemployment claim has been filed in their name, their identity has likely been stolen at some point in time. The affected staff should take additional steps to help protect their identity such as credit monitoring or identity theft protection services. Please also reach out to KDOL and report the identity theft.

Contact: Report UI Fraud to KDOL by emailing ronda.kirk@ks.gov or Nicholas.beech@ks.gov, If you have any questions or concerns, please contact Jeff Maxon at jeff.maxon@ks.gov

Attached: US Secret Service Alert on Massive Unemployment Fraud