

Bond Case Briefs

Municipal Finance Law Since 1971

Kronos Ransomware Attack Will Challenge Public Finance Issuers.

Fitch Ratings-New York/Chicago/Austin-21 December 2021: The recent breach of Ultimate Kronos Group's (UKG) Kronos Cloud Solutions platform could pose significant, but temporary, management challenges for public finance entities that use the Kronos platform through the holiday season, says Fitch Ratings. While we do not anticipate that the UKG breach will have meaningful credit implications for individual public finance entities that use Kronos, the breach continues to reinforce the necessity of robust third-party risk management strategies and identification of critical dependencies for public finance issuers. The attack further highlights the importance of cyber emergency preparedness and response strategies for the public finance sector.

The breach has already impacted a large number of public finance entities across the country, with some of the most notable the New York Metropolitan Transportation Authority, the City of Cleveland, the state of West Virginia, the Oregon Department of Transportation, the University of California system, and Honolulu's EMS and Board of Water Supply. Though many high-profile public finance organizations have disclosed being impacted, the actual number could be much larger.

UKG is the provider of one of the most popular and widely used payroll and workforce tracking systems for public finance entities. On Monday December 13, UKG announced that it was the victim of an ongoing ransomware attack affecting the Kronos Private Cloud, which hosts UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions. The company further disclosed that the Kronos Private Cloud solutions systems are currently unavailable and it may take up to several weeks to restore system availability for clients. The breach is forcing many issuers across the spectrum of public finance to resort to manually tracking and estimating employee hours, having to issue paper paychecks and possibly causing paycheck delays during the holidays.

The sector most impacted by the UKG ransomware attack within public finance is healthcare, where Kronos' payroll and workforce solutions systems have been popular. The breach should not affect clinical outcomes or add meaningful costs, except some added expenses activating contingencies to track hours and pay workers. That said, the timing is especially inopportune for the sector, with hospitals nationwide already grappling with increased Covid-19 cases amid the growth in the Omicron variant. Indeed, the American Hospital Association (AHA) stated that some hospitals and health systems have been impacted by this ransomware attack and urged all third-party providers that serve the healthcare community to examine their cyber readiness, response and resiliency capabilities.

In addition to the near-term challenges posed to public finance entities from the current unavailability of critical payroll systems, some entities have voiced concerns over data privacy associated with the UKG breach. According to a statement released from the City of Cleveland, some of the city data accessed may have included certain employees' first and last names, addresses, last four digits of the social security numbers, and employee ID numbers.

Contacts:

Omid Rahmani
Associate Director, USPF
+1 512 215 3734
Fitch Ratings, Inc.
2600 Via Fortuna, Suite 330
Austin, TX 78746

Greg Dziubinski
Associate Director, USPF
+1 312 606 2347
Fitch Ratings, Inc.
One North Wacker Drive
Chicago, IL 60606

Justin Patrie
Senior Director, Fitch Wire
+1 646 582 4964
Fitch Ratings, Inc.
Hearst Tower
300 W. 57th Street
New York, NY 10019

Media Relations: Sandro Scenga, New York, Tel: +1 212 908 0278, Email:
sandro.scenga@thefitchgroup.com

The above article originally appeared as a post on the Fitch Wire credit market commentary page. The original article can be accessed at www.fitchratings.com. All opinions expressed are those of Fitch Ratings.