U.S. Department of Justice
National Unemployment Insurance Fraud Task Force

Vulnerability Associated with Cyber Activity Against State Workforce Agency Unemployment Insurance Computer Systems

CONTROLLED: DISTRIBUTION LIMITED TO STATE WORKFORCE AGENCIES ONLY

January 11, 2024

Federal law enforcement agencies continue to see post-pandemic threats to state workforce agencies (SWAs) administering unemployment insurance (UI) programs. It is imperative SWAs employ a multi-faceted approach to fraud detection and prevention, using an array of controls, tools, strategies, and resources to identify and prevent fraud. States cannot rely solely on one identity verification service or fraud prevention solution to prevent and detect the numerous and evolving fraud schemes targeting the UI program. Federal law enforcement agencies have recently become aware of a growing post-pandemic trend by cyber criminals accessing SWA UI claimant and employer computer systems and web applications in order to:

- Establish new UI claimant accounts;
- Establish new employer accounts (fictitious employers);
- Overtake/access ("claim hijacking" or "claim/account takeover") pre-existing UI claimant accounts, including accounts of state government employees;
- Make changes to direct deposit information, often to banks with no in-state presence or routing numbers that correspond to other regions;
- Access pre-existing employer accounts, including accounts established by Third Party Administrators administering UI benefits for hundreds to thousands of employees, particularly in the healthcare industry; and
- Fraudulently file for pandemic and post-pandemic (regular) UI benefits.

Some affected SWAs have reported that cyber criminals initially accessed other state computer systems and then moved laterally to the SWA UI systems. SWAs and their information security personnel were able to demonstrate that cyber criminals rapidly accessed UI web applications—potentially through automation—and were able to readily defeat common knowledge-based identity verification tools. These events reinforce the need for a multi-faceted approach to fraud detection and prevention and why it is critical to not rely solely on one tool or service.

Cyber actors have been observed making hundreds of thousands of requests against UI web applications over brief periods. In some instances, cyber criminals appeared to possess specific internal field names from SWA UI databases. Further, law enforcement believes that cyber criminals have accessed personally identifiable information (PII) in SWA UI databases to file UI claims against the victim SWA, file claims against other SWAs, or use the stolen PII for other criminal activity.

Known losses are approximately $2 million but are anticipated to increase. Fraudulent activities are likely to increase when states launch new benefits or tax systems, announce and implement new processes or services (such as ID verification), and in times of increased workloads, (such as winter months or tax season).

The U.S. Department of Labor, Office of Inspector General (DOL-OIG) reminds SWAs that:

- Under the Inspector General Act of 1978, the Inspector General Empowerment Act of 2016, and various UI Program Letters, SWA disclosure of UI information to the DOL-OIG for investigative purposes is mandatory.

- SWAs are obligated to report alleged or suspected UI fraud, misfeasance, malfeasance, nonfeasance, waste and program abuse, mismanagement, misconduct, and other criminal activities to the DOL-OIG. As outlined in this alert, cyber criminals have engaged in multi-claimant, multi-state schemes involving identity theft as well as fictitious/fraudulent employer schemes involving multiple states and international boundaries. This activity must be reported to the DOL-OIG, regardless of the amount of suspected UI losses.

- When reporting UI information linked to this activity to the DOL-OIG, SWAs should include full PII of victim claimant(s), telephone number(s), email address(es), bank account(s) and associated internet protocol addresses linked to suspect claims identified.

- The DOL-OIG does not consider SWA reporting of suspected criminal activity through the National Association of State Workforce Agencies Integrity Data Hub as fulfilling SWA obligations to inform the DOL-OIG of significant UI fraud.

- Referrals or questions regarding this activity can be routed by SWAs to their local DOL-OIG Special Agent-in-Charge, or questions may be routed to DOL-OIG's National UI Fraud Coordinator, Senior Special Agent Brooks Abramson at abramson.brooks@oig.dol.gov.

Individuals with information about UI fraud should call (202) 693-6999 or (800) 347-3756, or go to https://www.oig.dol.gov/hotline.htm