

Unemployment Insurance

FRAUD, WASTE, AND ABUSE IN THE COVID-19 ERA

By Jon Coss, Vice President, Risk, Fraud & Compliance, Thomson Reuters Pondera



During the 12 months leading up to the country's coronavirus response, the Department of Labor estimated that improper payments accounted for 10.61% of just under \$31 billion in Unemployment Insurance (UI) benefits.

Then, suddenly, 33 million Americans applied for unemployment insurance in less than two months. This has driven the nation's unemployment rate to around 15%, the highest rate since the great depression.

The sudden surge in UI applications has overwhelmed state employment departments, many of which have waived certification and work search requirements. And while Program Integrity (PI) departments continue to work to protect the fiduciary trust put in them by businesses and citizens, they face an almost impossible task of reducing improper payments while not delaying applications and payments.

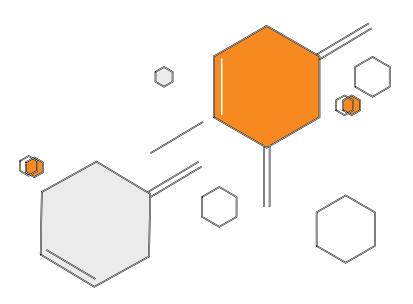


The current circumstances create a "target rich" environment for potential fraudsters, in addition to inevitable increases in waste and abuse. While states are rightfully focusing on processing applications and making payments, fraudsters now have more opportunities to "sneak through" the front door using stolen identities and other commonly used fraud schemes.

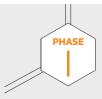
Several current factors make this a uniquely attractive environment to those who would defraud the government. The sudden surge in claims makes traditional program integrity methods almost impossible to administer without slowing down payments. And the additional \$600 per week in benefits provided by the Coronavirus Aid, Relief, and Economic Security Act (which doubles the average state benefit) will invite a greater volume of scammers. Even after the additional funding expires, successful fraudsters will continue to collect improper payments until they are identified and stopped.

Based on our experience with Fraud, Waste, and Abuse (FWA) in state UI programs, we expect to see the following three phases of improper payments over the next 18-24 months. Of course, there will be overlap between the phases. However, we expect to see this pattern based on our understanding of the unique nature of this financial crisis. In addition, this pattern will reflect previous unemployment cycles and associated UI scam types. The current circumstances create a "target rich" environment for potential fraudsters, in addition to inevitable increases in waste and abuse.





Some of these "two-sided" schemes are likely already in operation. The term "two-sided" refers to schemes in which both the employer and employee make use of stolen identities so there is no one who will tip off the state to the scheme. A second wave is likely to emerge over the summer and fall of 2020, after the fraudsters are able to "catch up" by creating fictitious businesses, registering them with employment departments, "hiring" employees, filing a false quarterly wage report, postponing payment of UI taxes, "firing" employees, and then filing false benefit claims.



Fraudulent First Time Claimants From present until return to normal claims volumes

Using stolen identities, fraudsters are filing, and will continue to file, first time and ongoing claims for UI benefits. We commonly see identities and Social Security numbers submitted from deceased, out-ofstate, and incarcerated individuals. We've also seen children and even foreign student identities used in UI fraud. These scams will be perpetrated both as "one-offs" and in "bulk".



Benefit – Wage Conflicts

From economy reopening until return to normal unemployment levels

Unlike any other sudden unemployment surge in our history, 83% of those filing new claims expect to get their jobs back within six months, as states re-open their economies. This will bring a second wave of fraud or waste as people return to work and fail to notify state employment agencies. Collecting benefits at the same time as earning wages has always been one of the most common abuses in UI, and the large volume of people returning to work in such a short period of time will dramatically increase overpayments.



Fictitious Business Scams

From summer 2020 until effective enforcement

Fraudsters regularly use fictitious businesses, which then hire and fire fictitious employees, to steal from UI programs. Even the fraudsters, however, were likely surprised by the rapid increase in unemployment brought on by COVID. Therefore, the full effects of these schemes will not be felt until the summer and fall of 2020.



We understand that state employment departments are playing, and will continue to play, a major role in supporting the economy and the economic reopening we all hope for. We also understand that this starts with the timely delivery of services and payments to those who need them. Any recommendations that we make must be considered in this context. Program Integrity, while important to the state employment programs and to businesses who pay into the state unemployment trusts, must not interfere with or delay the distribution of UI payments.

With this in mind, we recommend that UI Program Integrity Units consider the following recommendations to combat fraud, waste, and abuse during this historically difficult time:

Val

Validate New and Recent Claimants: Consider adding additional batch and/or individual lookup capabilities to validate a claimant's social security, deceased status, residency, and incarceration status. This could include using files like state incarceration and vital records, as well as systems from the Department of Labor and the National Association of State Workforce Agencies (NASWA). In addition, cross-matching identities against third-party data (from consumer data aggregators) is generally recommended here to reduce overpayments based on incomplete, incorrect, or latent government data files.

To identify more collusive (and thus higher risk) schemes, states should have the ability to rapidly identify shared applicant attributes such as addresses, emails, phone numbers, and Internet Protocol (IP) addresses. This will help already overburdened PI staff achieve higher ROI from single investigations.



Prepare for Wage-Benefit Overlaps: As economies begin to reopen and citizens go back to work, we expect a historically high number of wage-benefit conflicts. While traditionally viewed as waste, even a few additional payments spread across such a large number of people will result in a significant total outlay.

To address this, states should make sure now, ahead of the problem, that they have the ability to quickly identify claimants that have returned to work and continue to collect payments. In addition, they should consider automated notification and collection systems. This will allow busy PI staff to work on more labor-intensive processes, such as investigating potentially fictitious businesses.



Analyze New and Newly Active Businesses: While it is already a standard process in most employment agencies, we suggest that PI staff adequately review unemployment claims against new businesses (opened since the start of the epidemic) and previously dormant businesses. Clearly, this is not the ideal environment in which to open a new business or re-start a previously inactive one. Cross-checking the employers associated with claims against a list of recently opened or activated businesses will help reduce improper payments to purely fraudulent actors from whom it will be extremely difficult to recover funds post-payment.

Consider Implementing a Platform to Support Program Integrity: Implementing software solutions and processes for each of the discreet situations described in this paper will undoubtedly help state employment departments manage the onslaught of fraud, waste, and abuse that will accompany this unprecedented surge in unemployment claims. However, it is also highly unlikely that we will return to pre-COVID employment levels (and associated FWA) anytime in the near future.

To address both immediate and long-term program integrity requirements, states should consider implementing a software platform into which they can "plug" just-in-time analytics, and which will support their enforcement processes and reporting requirements. This will allow agencies to deliver immediate value to their states while also centrally managing the analytics required to fight FWA into the future.

It is important to remember that when fraud schemes are identified and shut down, bad actors do not suddenly become honest citizens. Instead they adjust their schemes and tactics and PI departments will need to keep pace with new and emerging fraud methods. A centralized, configurable platform will allow them to do this now and into the future.

Detect Sophisticated Fraud With an Integration Solution

Thomson Reuters and Pondera offer a number of fraud, waste, and abuse tools and systems to help you detect, prevent, and investigate unemployment insurance fraud. CLEAR® offers immediate batch identity validation and risk identification as well as nationwide incarceration verification and real-time lookup. Pondera offers a comprehensive analytics system that integrates CLEAR data, your claimant and employer data, as well as claims details to identify your highest risk claimants and employers to investigate. Advanced models and algorithms help you detect and prevent improper payments to stolen identities, out-of-state applicants, and employees who have returned to work, as well as complex fraud schemes and clusters of fraudulent claimants.

Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act (FCRA), 15 U.S.C. sec. 1681 et seq. The data provided to you may not be used as a factor in consumer debt collection decisioning, establishing a consumer's eligibility for credit, insurance, employment, government benefits, or housing, or for any other purpose authorized under the FCRA. By accessing one of our services, you agree not to use the service or data for any purpose authorized under the FCRA or in relation to taking an adverse action relating to a consumer application.



