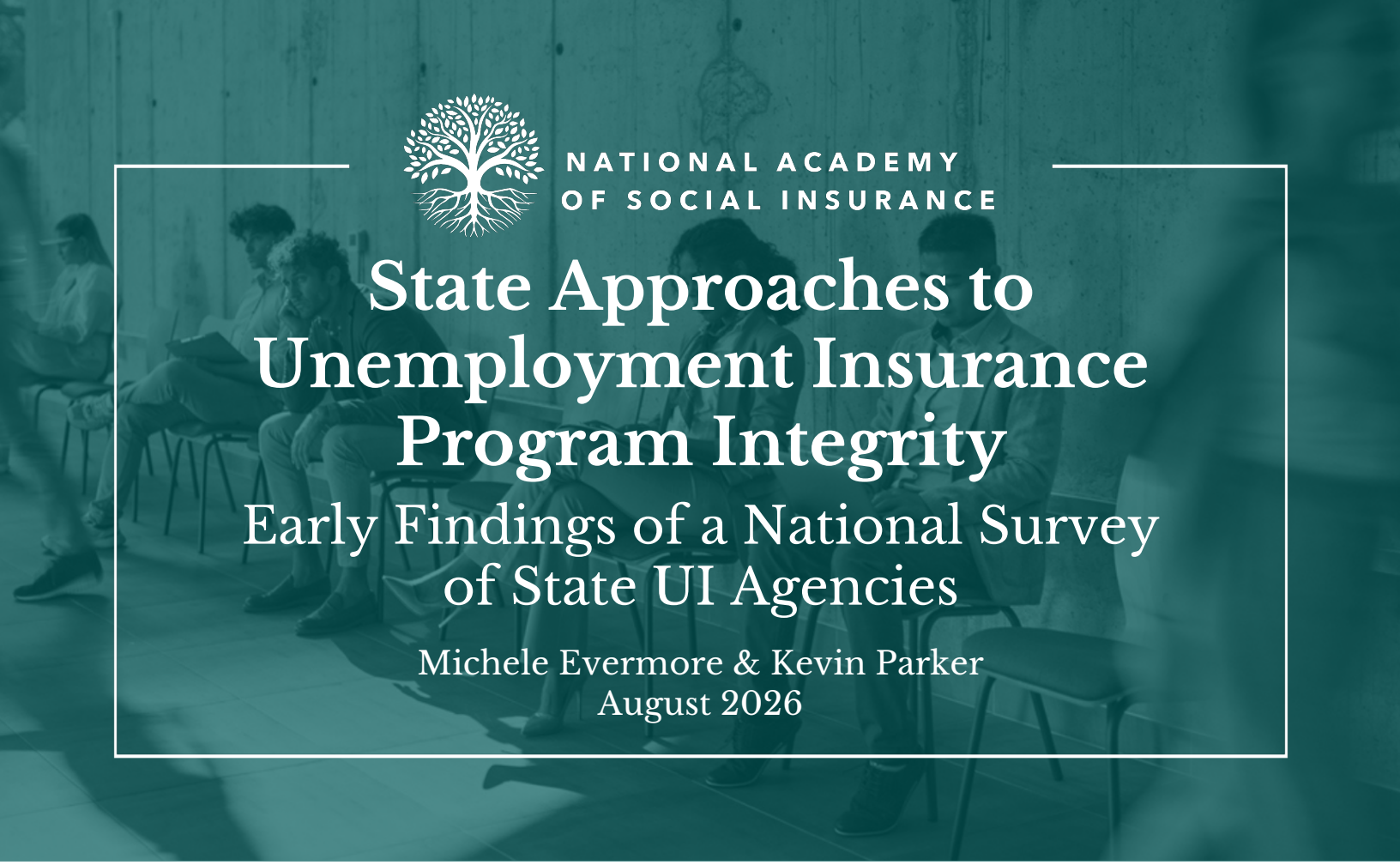

NATIONAL ACADEMY OF SOCIAL INSURANCE

State Approaches to Unemployment Insurance Program Integrity

Early Findings of a National Survey of State UI Agencies

Michele Evermore & Kevin Parker

August 2026

This brief presents early findings from a national survey examining how state unemployment insurance (UI) agencies are adapting their program integrity practices in response to evolving fraud risks and operational challenges. The project was conducted by the National Academy of Social Insurance in partnership with the National Association of State Workforce Agencies (NASWA), with support from Arnold Ventures.

Overview

UI programs across the United States continue to operate in a higher-risk high-frequency fraud environment following the unprecedented surge in fraudulent activity during the COVID-19 pandemic. In response, state agencies have significantly expanded fraud detection tools, identity verification systems, cybersecurity safeguards, and interstate data-sharing practices to strengthen program integrity while maintaining timely access to benefits for eligible workers.

To better understand how states are adapting to this environment, the National Academy of Social Insurance (NASI), in partnership with the National Association of State Workforce Agencies (NASWA), conducted a national survey of state UI agencies in early 2026. The survey examined current practices related to fraud prevention, detection, identity verification, cybersecurity, overpayment recovery, and program administration.

All 53 states were invited to participate in the survey. Valid responses were received from 34 state cross all six administrative regions. The UI programs from these states vary widely in size, technology systems, staffing levels, and administrative structure.

The findings from this survey provide one of the most comprehensive post-pandemic snapshots of how states are addressing program integrity challenges across the federal-state UI system.

The survey results indicate that program integrity has become a permanent operational responsibility within the UI system, requiring sustained investment in technology, staffing, and interstate coordination.

Key Findings

Survey responses revealed several consistent patterns across states despite substantial differences in program size, technology systems, and administrative structure. Six major themes emerged.

- Fraud is now a persistent operational condition. State agencies consistently report that fraud is no longer a temporary spike associated with pandemic programs but an ongoing operational challenge driven by identity theft, automation, and organized fraud networks.
- States are detecting more fraudulent claims before payment. Many states report identifying a majority of suspected fraudulent claims prior to payment, reflecting expanded use of identity verification, automated fraud analytics, and cross-state data-sharing tools.
- Identity theft remains the dominant fraud strategy. The most frequently reported fraud activity involves stolen personal information used to file claims or gain access to existing claimant accounts.
- Identity verification has become the primary front-end safeguard. Most states now use identity verification as a core part of the claims process, either universally or through risk-based models designed to prevent fraudulent payments before they occur.
- States' vigilance about identity fraud have dramatically reduced payment to bad actors and identity thieves.
- Program integrity capacity varies significantly across states. Differences in technology systems, staffing levels, vendor partnerships, and administrative structures affect how effectively states can prevent, detect, and recover improper payments.
- Sustained investment is required to maintain current integrity levels. States consistently report that maintaining current fraud prevention and detection capabilities requires ongoing funding, staffing, and modernization of technology systems.

The Current Fraud Environment

Survey responses indicate that the fraud environment facing UI programs has changed significantly since 2020. Pandemic-era programs exposed vulnerabilities in eligibility verification, identity authentication, and system security. Although claim volumes have stabilized, fraud attempts have not returned to pre-pandemic patterns.

States consistently report that fraud is now:

- More organized
- More automated
- More likely to involve stolen identity data
- More likely to occur across multiple states simultaneously

Many respondents described fraud as a standing operational condition rather than an emergency event. Fraud today is organized, automated, and continually adapting to new safeguards, requiring ongoing prevention efforts rather than one-time responses.

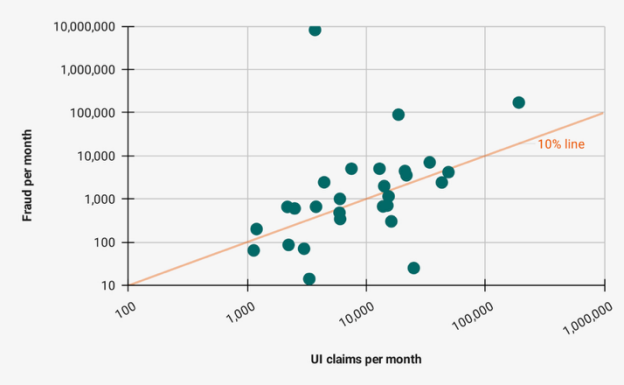

Figure 1: Variation in UI Claim Volume and Suspected Fraud Across States. Each data point represents one state. The number of UI claims and the number of fraudulent claims are plotted on a logarithmic scale. The diagonal line marks where the states below the line have less than 10% of the total UI claims flagged as fraudulent.

Organized and Multi-State Fraud Activity. States reported evidence of coordinated fraud networks using stolen personal data, automated claim-submission tools, and distributed infrastructure to target multiple UI systems at the same time. These patterns underscore the importance of interstate data-sharing tools and federal coordination.

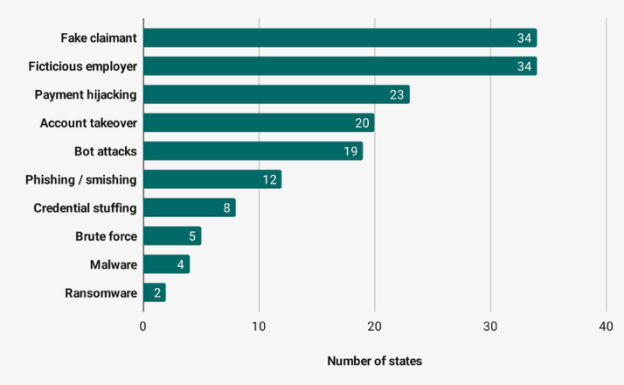

Figure 2: Most Frequently Reported Fraud Activities in UI Programs. All responding states reported experiencing at least 2 and most commonly 4-5 different types of fraud activities in the past year. Fake claimant identity and fictitious employer are two most frequently reported types of fraud.

Identity Theft as the Primary Threat. Identity theft remains the most frequently reported fraud activity. Fraud actors use stolen Social Security numbers and personal information to file claims or take over existing accounts. Several states also reported increased attempts to redirect payments after claims are approved.

Fraud Tactics Continue to Evolve. Fraud activities are becoming more premeditated and elaborate to evade detection. States described emerging tactics including:

- Automated claim submission
- Creation of seed accounts ahead of time

- Credential-harvesting and phishing attacks
- Fictitious employer schemes
- Bot activity targeting claimant portals
- Attempts to bypass identity verification
- Usage of artificial intelligence

Respondents emphasized that as safeguards improve, fraud actors adjust their methods, requiring continuous system updates.

Integrity as an Ongoing Operational Function. States consistently reported that fraud prevention now requires permanent investment in technology, staffing, cybersecurity, and collaboration with other entities. Agencies indicated that without sustained support, integrity gains made since the pandemic could be difficult to maintain.

How States Are Strengthening Fraud Detection

States report significant expansion of fraud detection tools since 2020. Common approaches include:

- Automated fraud analytics
- Identity verification vendors
- Cross-match databases
- Interstate data-sharing systems
- Dedicated investigative staff

Many states reported that they now flag a majority of suspected fraudulent claims before payment is issued.

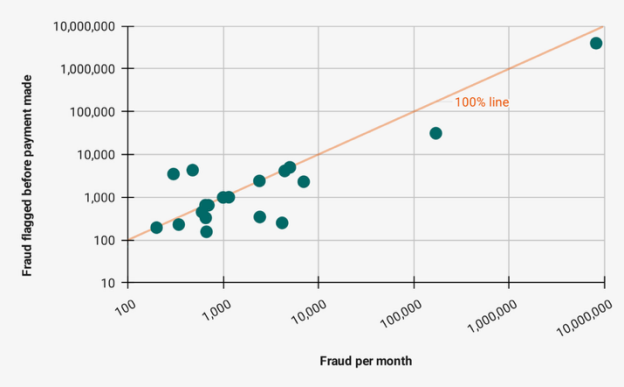

Figure 3: Share of Suspected Fraud Detected Before Payment. Each data point represents one state. The number of fraudulent claims and the number of fraud flagged before a payment is made are plotted on a logarithmic scale. The diagonal line marks where the states below the line have less than 100% of the fraud activities flagged before a payment is made.

Manual review is a bottleneck in integrity workflow. Earlier detection reduces improper payments but increases workload, because flagged claims must be reviewed manually. Several states noted that improved detection systems require sufficient staffing to avoid delays in processing legitimate claims.

UI fraud is dynamic environment. As safeguards improve, fraud actors change tactics. States emphasized that stronger detection often results in more fraud being identified, but not fewer fraud occurrences. Stronger detection must also be balanced with potentially false positive alerts. States are exploring ways to leverage emerging technologies to update detection algorithms and increase the signal-to-noise ratio.

Prevention is the key. Early detection does prevent fraud-related overpayment. Although most states reported that bad actors are responsible for the majority of fraud, only a small portion of the states' overpayment went to bad actors. NASI's recent congressional testimony also noted that

prevention provides the strongest return on investment in UI program integrity. Every dollar prevented before payment avoids downstream recovery costs.

Why UI Program Integrity Remains a National Priority

The pandemic demonstrated both the importance of the UI system as a safety net for workers and families, and the risks created by outdated technology and limited administrative capacity. During the crisis, more than 53 million people received benefits, helping stabilize the economy during an unprecedented downturn.

At the same time, the surge exposed long-standing weaknesses in administrative funding, technology systems, and staffing. States entered the pandemic with historically low administrative funding and limited modernization resources.

The challenges the states faced during the pandemic — battling fraudulent claims while ensuring that legitimate claims are processed in a timely manner, and recovering overpayments — have been well documented. However, it has been unclear how the UI fraud landscape has changed since the pandemic and how the state agencies are responding.

This national survey tries to answer these questions. Today, state UI agencies report that:

- Attempts of fraud continue even at normal claim levels
- Organized crime targets multiple states
- Technology modernization remains uneven
- Staffing constraints limit investigative capacity

Because UI is a federal-state system, differences in state capacity can create vulnerabilities that affect the entire program. Maintaining integrity therefore requires coordination among various entities including state agencies, Federal partners, vendors, financial institutions, and policy organizations. Effective integrity efforts must protect taxpayer dollars while ensuring that eligible workers receive benefits on time.

Key Considerations for Policymakers

Findings from this nation-wide survey of state UI agencies suggest several areas where continued attention may be needed:

- Sustained funding for program administration
- Support for identity verification and fraud prevention tools
- Investment in technology modernization
- Expansion of interstate data-sharing systems
- Improved data reporting and consistency
- Continued federal-state collaboration on integrity efforts
- Fraud assisted by AI is growing more sophisticated

Program integrity in the UI system means paying the right person the right amount at the right time. Efforts that prevent fraud but delay benefits to eligible workers do not fully achieve that goal. Maintaining both accuracy and timeliness will remain a central challenge for the UI system in the years ahead.