IMPROVING THE FEDERAL UNEMPLOYMENT INSURANCE SYSTEM

By Gregg Tahmisian
CEO

SOLIDSTATE

> The nature of demand for unemployment insurance system services is often sudden, unpredictable, and occurring during rapid economic changes.

Due to structural design and state law variations, unemployment insurance is a remarkably complex program to administer.

Economies of scale that might be achieved in other settings are more difficult in the UI federal- state partnership model which emphasizes state autonomy in both statutory program design and IT investment choices.

UI systems must serve varied stakeholders (with differing interests and needs) on both the tax collection and benefit administration fronts. The nature of demand for unemployment insurance system services is often sudden, unpredictable, and occurring during rapid economic changes.

Funding for IT or system upgrades has traditionally been lower than needed and/or inconsistent, and often, especially during times of low unemployment, these sums are leveraged for other state priorities.

After a crisis, additional investment is made in reaction to the system's performance failures, but sustained investment or maintenance costs are not usually included. The collective weaknesses of these realities have been in stark relief over the past year and there is certainly room for improvement across the UI technology spectrum: structural changes, system changes, and application-specific changes.

From Solid State Operations experience with states and unemployment insurance technology, there are several recurring themes that could inform the Department's approach to additional investments.

1. **CENTRALIZE USER EXPERIENCE.** Unemployment insurance has, by definition, multiple end users: state workforce agencies, employers, and claimants. Improving any of these users' experiences is rarely a top priority in UI system design.

2. **INCREASE AUTOMATION TO REDUCE STRAIN ON STATE STAFF.** One of the most significant sources of UI program inefficiency is the frequency with which a state agency employee must interact with a claimant to resolve issues. Some of the causes are programmatic or structural, but many are likely preventable with more up-to-date design and communication standards.

3. **PLAN FOR DATA SHARING.** The inability to safely and quickly share UI data to provide insight to other relevant parties (including for law enforcement, other state government agencies, and claimant support resources) creates recurring complexity and drains state staff time.

4. **DEMAND BASELINE SECURITY POSTURES.** States have not kept pace with standard security protocols and are often easy targets for even low-sophistication fraudsters. The Department or an approved third party could define baseline security standards to reduce fraud. States should be evaluated against technical security specifications as part of their UI performance evaluation and reporting requirements.

5. **GRADUALLY CHANGE NORMS.** Historically many state workforce agencies (and the legislatures that fund them) and related teams have viewed UI investments as "deploy and forget" rather than adopting continuous change models of incremental improvement.

6. **SIMPLIFY PROCUREMENT AND EXPAND VENDOR POOL.** Due to often-painful procurement structures and the niche market, the UI vendor ecosystem is fairly limited. The vendor ecosystem might be more diverse if procurement were simplified, and interoperability or standardization allowed states to reuse or share component parts of systems. Additionally, states should use outcomes-based or alternate payment structures to properly align incentives for states and vendors.

The role of the Federal government in the UI system has varied over time, but we see three clear areas where additional Federal clarity would be helpful to both states and the vendors that support them:

- Standards: defining a complete UI system, defining basic security standards, defining identity validation, data taxonomy, data sharing and reporting expectations, etc.

- Procurement: providing some elements to states via common platform infrastructure; subsidizing SaaS subscriptions for approved platform-aligned software or services; encouraging development of dynamic vendor ecosystem with procurement assistance services or examples of creative, incentive payment structures.

- Technical Evaluation: in addition to monitoring benefit accuracy and timeliness, there may be some role for additional technical oversight to ensure that state systems do provide the basic capabilities and can comply with stated standards.

1. CENTRALIZE USER EXPERIENCE

The unfortunate reality is that the claimant interfaces to State UI systems are usually woefully inadequate and outdated. And as the interface between the workforce agency and an extremely diverse group of claimants, the claimant portal must be accessible to people of different abilities, ages, languages, proficiency, internet devices, and technological sophistication.

Many States lack this sort of substantive, accessible claimant portal. They are missing key pieces of functionality, contain instructions which are not presented in users' languages, are difficult to understand, do not allow representatives to assist claimants, contain significant accessibility barriers, and/or appear to be untrustworthy by claimants. Beyond that, few states have claimant portals that can handle complete full fact finding, appeal management, or online document management with a secure message center. Equitable benefit delivery requires significant investments in and commitment to accessibility in all its forms; at the center of that investment is user-centric design.

For states to handle UI spikes, they must push usable, self-serve functionality to the claimants on various mediums. This is crucial for reducing staff time spent dealing with paper processing, in-person questions, or contact center phone calls. Staff hours should be optimized for the most difficult and non-automatable tasks; this is more possible when users can solve more problems on their own.

Claimants are, of course, not the only stakeholders required to interact with the UI system – employers, state workforce agencies, and relevant third parties are also needed for the UI system to function smoothly.

Gathering user feedback from these groups and designing with them in mind would alleviate many of the less publicly visible burdens of UI system design.

2. INCREASE AUTOMATION TO REDUCE STRAIN ON STATE STAFF

Self-service functionality. This should be the objective of modern user-centric applications such as a claimant portal, employer portal, or adjudication module. Giving users the ability to self-serve allows them to accomplish tasks more quickly with less hassle and friction and saves staff time. Claimants benefit when given the ability to accomplish tasks online such as: updating personal info, updating banking info, submitting documents online, providing answers to fact finding questions, etc. Likewise, employers benefit from self-service functionality such as verification of claim info and providing answers to fact finding questions without a complex interaction with the state workforce agency.

System availability: Many state UI systems are only functional during "business hours" (often around 7:00AM to 5:00PM local time). This is because the older mainframe systems shut down at night for "processing," and online systems shut down around the same time. This creates a potential inconvenience for claimants and a bottleneck in the system as all claims have to be filed in a smaller time window. Additionally, the inability of the UI systems to operate around-the-clock causes a lack of trust in the UI system. Public perception is that if the UI system cannot perform even as well as the most rudimentary ecommerce site, it probably is not trustworthy. Deficits in public trust translate to exponential pressure on the State executive branch in times of crisis; working to rebuild that trust in non-crisis time requires at least ongoing system availability.

Communication: Many UI systems still communicate primarily via paper correspondence. Mainframe systems were put in place before the age of cell phones and email. As these technologies have taken over modern life, UI systems have not kept pace. Most UI systems do not use text messages (SMS).

Going forward, UI systems need to communicate with claimants and employers using a variety of methods, and users should be able to indicate their preference for method. Allowing users to go "paperless" allows claimants to get information in the way they prefer, and states save money in postage. It is unrealistic to expect that customers will constantly log back into the UI system to check for updates, but many systems expect this. Pushing information out through email, text, or mobile applications allows customers to choose which method works best for them. Systems should strive to minimize the use of mailed documents; if it is required by law, that should be made clear to customers.

3. PLAN FOR DATA SHARING

UI benefit administration requires data sharing across the entire lifecycle of a claim: verifying separation situations, obtaining wage records, connection to reemployment services as applicable, or even assisting law enforcement in fraud prosecution. On an individual level, claimants often need help for their initial or continuing claim management. A read-only view of claim status could help claimants who are working with other state agencies or need to share info with a legal aid representative.

On a macro level, the system should be able to share data easily, safely, and securely with other state and federal systems. Examples of this technology coordination include single-sign on, income verification for self- employed and gig-economy workers, crossmatches for fraudulent or invalid claims, IRS tax intercepts, benefits withholding for child support, interstate claim reporting through ICON, etc.

Interoperability is a Systemic improvement because there needs to be standardization across the interfaces that systems use to communicate. A Federal platform or, at the least, a standardized data sharing or secure communication platform could reduce the friction in finding and using relevant data quickly to speed benefits to eligible claimants and prevent benefits from reaching fraudsters.

4. DEMAND BASELINE SECURITY POSTURES

Identity Proofing and Management: During the pandemic, most of the wholesale fraud schemes relied on fraudsters identifying themselves to the UI system as a person they were not. Fraudsters employed bots to file massive numbers of SSNs against state UI systems, using stolen information available on the dark web. Nearly all of these could have been stopped by rigorous identity proofing, which simply means verifying that the person using the system is who they claim to be. There are various providers that perform this service, usually by asking the claimants information that only the claimant should know, such as "Which of the follow make/model of car was ever associated with you." Any one of these multiple-choice questions could be guessed, but statistically, fraudsters should not be able to guess the correct answer to many of these questions.

Unfortunately, these identity services produce a high number of false positives (i.e. they flag a person as fraudulent when in fact they are who they claim; they just forgot e.g. what car they drove in the past.) Positive hits require work to verify the claimant's identity by some other means – usually a phone call from a call center agent. During the pandemic, states did not have enough call center agents to make the necessary phone calls to check each hit.

Sometimes states made the choice to ignore the hits and pay the claims anyway; sometimes the states decided to leave the identity issue pending (and stopping payment) on all the hits indefinitely. In the first case many fraudulent claims got through due to lack of identity proofing. In the latter, all the false positives simply idled (often for many months) until adjudication, and claimants were rarely told the issue preventing payment on the legitimate claim. Neither outcome is good.

Because of the nature of identity proofing, it is likely that false positives are unavoidable. States need a scalable model for providing rapid credential checking services for all positive hits generated by an identity proofing service. This service should have a visual component for checking identification documents – it could be either over video, or in person. The service should be scalable in the sense that more agents should be able to be added in times of high unemployment and removed during times of low employment. Because of the nature of government employment and the difficulty in rapid changes in workforce size, it is likely that vendors would be in the best position to supply this service and the underlying framework.

As a side note, accurate identity proofing is an essential prerequisite for more automated self-service. When done properly, secure self-serve features make the system more user-friendly, allows automation to speed claim processing, and frees staff time of other activities.

Access Management: Many states are still using outdated authentication schemes for claimant logins. Most of these are managed internally by either the State or a UI vendor. They rely on a username like a social security number or an email address as well as a short password or PIN. There are several problems with these home- grown authentication schemes:

- Easily compromised insecure passwords. Where passwords are too short, they can be compromised by brute force attacks. Where initial passwords are assigned by the state using claimant data (e.g. SSN, DOB, etc.) they can be easily guessed by attackers with access to claimant personal information. Even with more complex passwords, relying on single factor authentication to prove that the claimant identity is inherently more susceptible to attack. Passwords can be compromised by on a large scale by techniques such as credential stuffing, phishing, and password spraying. The most immediate solution is Multi-Factor Authentication (MFA) in the login process. While not perfect, MFA is inherently more secure than Single Factor Authentication; very few state systems require, or even allow claimants to utilize MFA in the login process.
- Byzantine password reset processes: In many cases, resetting passwords is arbitrary (it happens when the user does not request it, locking the user out of the system), it is onerous (requiring the user to call in to the agency, wasting user time and staff time), and/or inefficient (the password needs to be mailed to the user, which wastes time and postage).

Supporting Document and Signature Security: Supporting documentation includes anything which helps verify the claimant's identity, income, employment, or conditions of separation. Many UI systems do not allow online document uploads, or if they do, the capability is restricted to uploading certain types of files: image file types, word documents, PDFs, etc. Restricting upload to certain definitions of file type limits mobile-only users and any users without scanning equipment. Such limitations affect disadvantaged groups and leads to inequitable benefit outcomes.

For supporting documentation, claimant portal applications should allow photographs and scans of documents to be easily submitted. Most mobile banking applications allow users to submit photos of checks from their phones using the camera feature, and UI systems should allow this same level of flexibility in submitting documents online.

For documents requiring signature, some states still mail documents to clients. Mailing documents can be unreliable, time consuming, and expensive. And requiring claimants to physical sign and mail documents back compounds the problem. Instead, claimant portal applications should be designed to accommodate secure electronic signatures. Even having claimants upload signed documents creates unnecessary work and delay as staff must manually review uploaded documents. Many commercial applications utilize electronic document signing, and UI applications should follow suit.

Fraud Prevention:
During the pandemic, the UI system was exposed to a level of intentional, malicious, organized criminal attacks it had rarely seen before, and was found unprepared for the onslaught. The inability to detect and prevent these attacks cost the UI system billions of dollars in fraudulent claim payments. States were caught off-guard by the assault on their UI system and lacked the ability to prevent the massive fraud that ensued. Criminals filed enormous numbers of fraudulent claims using stolen personal information in multiple states. The accounts used fictitious information and directed payments to the bank account or address of the criminals. Criminals set up "phishing" websites that mimicked state systems in order to get claimants to enter their username/password into the fictitious site. Once they did that, criminals would use the information the claimant entered on their site to log into the authentic site and change the claim payments to go to the criminals' accounts or addresses.

Solutions can include a modern, secure login such as OpenID Connect with MFA will prevent the phishing, brute force, password spraying, or credential stuffing attacks. Implementing better identity proofing will help secure the system against wholesale identity theft. Better communication and data sharing agreements with other agencies would allow systems to detect duplicate claims and suspicious actors.

Although technologies to identify and stop these types of attacks exist and are used by the nation's largest banks, retailers, and other institutions handling massive payments, DOL was not able to ensure that states measured up to a common security standard to stop the most preventable intruders.

DOL should also encourage or require States to implement their own rigorous, responsive fraud analytics as a backstop. The combination of secure logins and rigorous identity proofing will dramatically reduce systemic fraud. Nonetheless, States would be well advised to maintain an adaptable fraud scoring system that has configurable identification criteria and weighting and allows the state to identify potentially fraudulent claims. Once identified, the States should have a well-defined process for closing the security hole that allowed the fraudulent issue to enter the system.
One important caveat to this recommendation is that any systems that are put in place to identify and prevent attacks must be designed to have minimal impact on legitimate claimants. This is true for two reasons:

1. Failing to pay legitimate claimants in a timely manner creates an undue hardship for affected claimants, defeats the purpose of legislative efforts, and reduces trust in state executive branch and the Federal UI system
2. States that rely on measures that adversely impact legitimate claimants will face strong pressure to turn off those measures during times of high unemployment to get legitimate claimants paid more quickly. This opens the state to attack at a critical time. For example, at the beginning of the pandemic, there was great pressure to ensure that as many claimants as possible got paid as quickly as possible. The approach to identity proofing in some states was not efficient and adversely affected legitimate claimants. In the rush to get claimants paid, some states left themselves vulnerable to attack by turning off identity proofing to expedite payment. Other states turned off strict proofing because they did not have the staff bandwidth to verify identity for the vast number of applicants flagged by the identity proofing process.

5. GRADUALLY CHANGE NORMS

Flexibility: During times of high unemployment and especially when new UI programs are added, rules can change quickly. Many systems lack an ability to adapt to these changing rules or new programs. UI systems were heavily criticized during the Great Recession and the pandemic for being slow to implement programs and pay benefits. These systems often required weeks or months of reprogramming to adapt to the changes and begin paying benefits, and this delay hindered the ability of lawmakers to get benefits in the hands of claimants as quickly as they intended. These delays put unnecessary burden on claimants and diminished the credibility of State governments and the UI program in general.

The programming tools and support available to modern languages, including IDEs, test frameworks, version control, DevOps support, etc. make them much more productive and thus easier to change quickly.

Architecture patterns such as relational databases, code modularization, service-based architecture, etc. make programming changes less risky, easier to test, and faster.

This is not to say that UI technology is simple. To the contrary, it is full of deceptively complex business rules, data structures that make data conversion and coding difficult, and webs of connected systems (internal and external) in order to function. Many of the complex business rules are actually driven by state law or regulation, and as state agency staff have learned those complexities over time, it is often very difficult to propose straightforward modern system solutions.

Expect to Scale: In March 2020, UI systems experienced a 1000% - 3000% spike in claims activity. Mainframe systems and even on-premise client-server systems had a very difficult time dealing with these loads. Scaling is a system's ability to dynamically add processing power to accommodate changes in load. Scaling is largely taken for granted by enterprises operating in a cloud environment, but since most UI systems do not operate in that environment, scalability for UI systems has been, to say the least, a challenge. In order to have a robust UI system, that needs to change. Systems should be modular, independently deployable, and independently scalable. Technology to achieve this goal is mature and well within reach of system designers. Containerization technology such as Kubernetes – which is baked into the major cloud providers such as AWS and Azure – is a very easy way to leverage not only instant scalability, but also application healing and easier deployments.

Continuous improvement: Rather than "deploy and forget" agencies need to solicit feedback from customers, representatives, and front-line staff. Continuous feedback allows for continuous improvement. UI systems are so complex and ever-changing that no one has them implemented perfectly at any given time. Some states are already doing this well: Washington, for example, used customer surveys to inform its decisions about business process changes. New Mexico did a particularly thorough job with the usability surveys it sent to claimants and employers. Be sure to dig deeper than just asking customers for their overall level of satisfaction with the experience. Provide the opportunity for feedback at every stage, not just at the end of a transaction, by which point customers may have forgotten exactly what language they found confusing or where they got stuck. Create a mechanism for staff to provide suggestions for improvements as well and follow up in a timely manner. Without collecting ongoing feedback on systems, they will deteriorate.

Agencies need proactive assessments and continuous monitoring of the adequacy of State technology capabilities. This might best come through a consortium of representatives from State agencies, Federal agencies, vendors, and other stakeholders. This group could provide guidance on standards for evaluating the adequacy of systems, the evolving definition of interfaces between services, and systems best practices. The model for this type of governing body is the W3C body that governs internet standards.

6. SIMPLIFY PROCUREMENT AND EXPAND VENDOR POOL.

The state procurement process is fundamentally unsuited to procuring a complex system like UI software. UI systems are not a commodity like tires; states cannot describe a UI system with a code like "225/65VR17 M+S." Yet that is what state procurement rules expect state workforce agencies to do with UI systems. States have to describe exactly what they want with UI systems in order to buy them. They generally have to procure from a single vendor meaning that there are only a few vendors that can provide a complete, end-to-end UI system. This limits choice and often produces both lower quality and higher cost.

Agencies generally pay for systems up-front or in milestones. Based on the idea of focusing on outcomes, it would be much better for agencies to push risk onto the vendor by only paying for systems once they successfully go live. This puts motivation on the vendor to also focus intently on the ultimate outcome: quickly completing products to the agency's satisfaction.

Modular systems will produce modular contracting which will increase competition, producing better features and lower cost. The modular SaaS model of procurement lends itself to these goals. The "Salesforce model" is where one overarching agency purchases a blanket amount of platform services, and beneficiary agencies can avail themselves of services from various vendors who supply content modules on the platform. Using this model, the Federal government could procure the UI platform and the states could select the various completed content modules a la carte.

A modular, open framework for deploying UI applications would provide a definition of what general components constitutes a UI system (e.g., Tax, Benefits, Appeals, Adjudication, Federal Reports, ICON, etc.), as well as a definition of the interfaces between to components. Additionally, the framework would define services that could be used by all of the components (e.g., Print a document, Check for permission, Send notification to claimant, Verify claimant identity, etc.) Each component deployed on the platform would not have to reinvent the implementation of the other components or services. This allows any vendor to plug in their own content modules and know that they will inter-operate smoothly with all of the other components and services on the platform.

This type of standardization does not mean that every state needs to use the same content modules, but it does mean that content modules are standardized and interoperable so that vendors can develop content modules in a uniform, cost-effective way; and agencies can choose the modules that best fit their needs without having to worry about rearchitecting their infrastructure. This type of standardization also promotes reusability. A module developed by or for one agency can be supplied, theoretically without any modification whatsoever, to another agency. This reuse promotes robust feature development and lower cost for the agency.

SOLIDSTATE

www.solidstateops.com

solutions@solidstateops.com