DATA MANAGEMENT, ANALYTICS & VISUALIZATION

NC DEPARTMENT OF COMMERCE, DIVISION OF EMPLOYMENT SECURITY

UNEMPLOYMENT INSURANCE FRAUD

FRAUD DETECTION AND PREVENTION THROUGH THE POWER OF DATA AND ANALYTICS

INITIATED JANUARY 1, 2021
COMPLETED JUNE 31, 2021

Raju Gadiraju
NCDES Chief Information Officer

984-236-5769
raju.gadiraju@nccommerce.com

EXECUTIVE SUMMARY

As tens of millions of Americans lost employment as a result of the COVID-19 pandemic, state agencies responsible for delivering unemployment benefits faced many challenges, including new threats of widespread fraud. This submission highlights how the North Carolina Division of Employment Security (DES) and the North Carolina Department of Information Technology partnered in the use of data management, analytics and visualization to prevent and detect unemployment fraud in the wake of the COVID-19 pandemic.

- o **The Idea:** Implement a multi-layered technology solution incorporating data analytics and artificial intelligence to identify suspect behavior and offer insights in the fight against unemployment benefits fraud.
- o **The Implementation**: Leveraging internal and partners' capabilities, DES deployed a multi-layered solution consisting of Enhanced Secure Login, the DES Fraud Rules Creator, the GDAC Fraud and Identity Theft Solution, Enhanced Identity Verification, Enhanced Data Checks, and Enhanced Processes and Awareness.
- o **The Impact:** DES implemented a solution that helps reduce fraud, thereby saving taxpayer dollars, preventing criminal activity, and protecting the integrity of the unemployment benefits program. Other states may adapt and adopt this model to be better prepared to fight fraud in future economic downturns, natural disasters or emergencies.

IDEA

Since its creation in 1935 during the Great Depression, the nation's unemployment benefits program has provided critical financial support to individuals and communities during times of economic hardship. However, no economic downturn, natural disaster or emergency has tested states' abilities to administer the program like the COVID-19 pandemic.

Rapidly rising unemployment led to unprecedented claims volumes and vast new challenges for the North Carolina Division of Employment Security (DES). In March 2020, claims for unemployment benefits skyrocketed from approximately 3,000 a week to more than 20,000 a day (over 650%). DES worked to quickly pay out benefits to eligible claimants, ultimately issuing $14 billion in assistance to more than one million North Carolinians during the pandemic.

Unemployment benefits were administered on a larger scope and scale than in any other time in history. The federal government established new pandemic unemployment programs, expanded eligibility guidelines to include self-employed workers and those out of work due to COVID-19, and made large sums of federal funding available to states to distribute.

Unfortunately, these factors made state unemployment systems a prime target for fraudsters, and estimated unemployment fraud rapidly mounted to billions of dollars nationally. Historically, the majority of unemployment fraud involved individuals claiming benefits after they returned to work or providing false information on their applications. The pandemic introduced more sophisticated schemes involving mass filings of fraudulent claims, identity theft and imposter fraud, the hijacking of claimant accounts and bot attacks on online systems. While states have for years collaborated with the National Association of State Workforce Agencies (NASWA) to combat fraud, the traditional solutions and processes were not adequate or mature enough to combat the emerging techniques used in the pandemic.

In response, DES set out with a sense of urgency to implement a multi-layered technology solution that would incorporate data analytics to prevent and detect fraud in North Carolina's unemployment benefits system.

To more aggressively address fraud, DES leveraged its internal capabilities and partnerships to build new solutions expeditiously. A key partner is CapGemini, the contractor that implemented and manages SCUBI, the modernized online unemployment benefits system created for the consortium of North Carolina and South Carolina. Another is the N.C. Government Data Analytics Center (GDAC), which collects and analyzes information from various state agencies and is managed by the N.C. Department of Information Technology (NCDIT).

DES identified potential gaps in necessary data for fraud analysis and what entities would have the appropriate data to help fill them in. This is an iterative process – for example, GDAC has data sources available for DES to analyze, and based on that analysis artificial intelligence can be further developed and new features and functionalities can be integrated into SCUBI. Similar exercises can be conducted based on data available from NASWA or other data owners. The resulting fraud

detection solution allows for crossmatching of data from various sources, based on the assumption was that no one data source is 100% accurate in identifying an unemployment claim as fraudulent; however, if multiple sources identified suspicious indicators on a claim, the likelihood of fraudulent activity increases significantly.

DES takes a lead role in sharing its fraud prevention efforts with other NASWA member states to provide a model that they could adapt and adopt to help shore up their fraud prevention capabilities.

IMPLEMENTATION

DES's unemployment fraud solution was implemented as a multi-layered set of modular services allowing for crossmatching of data from various sources, with some overlap between the services. The underlying assumption was that no one data source would be 100% accurate in identifying an unemployment claim as fraudulent; however, if multiple sources identified suspicious indicators on a claim, DES would be able to identify fraud with a higher degree of certainty. Under this modular, multi-layered approach, DES deployed the six components below incrementally with no interdependencies.

North Carolina Unemployment Insurance Fraud Detection Prevention Solution Schematic
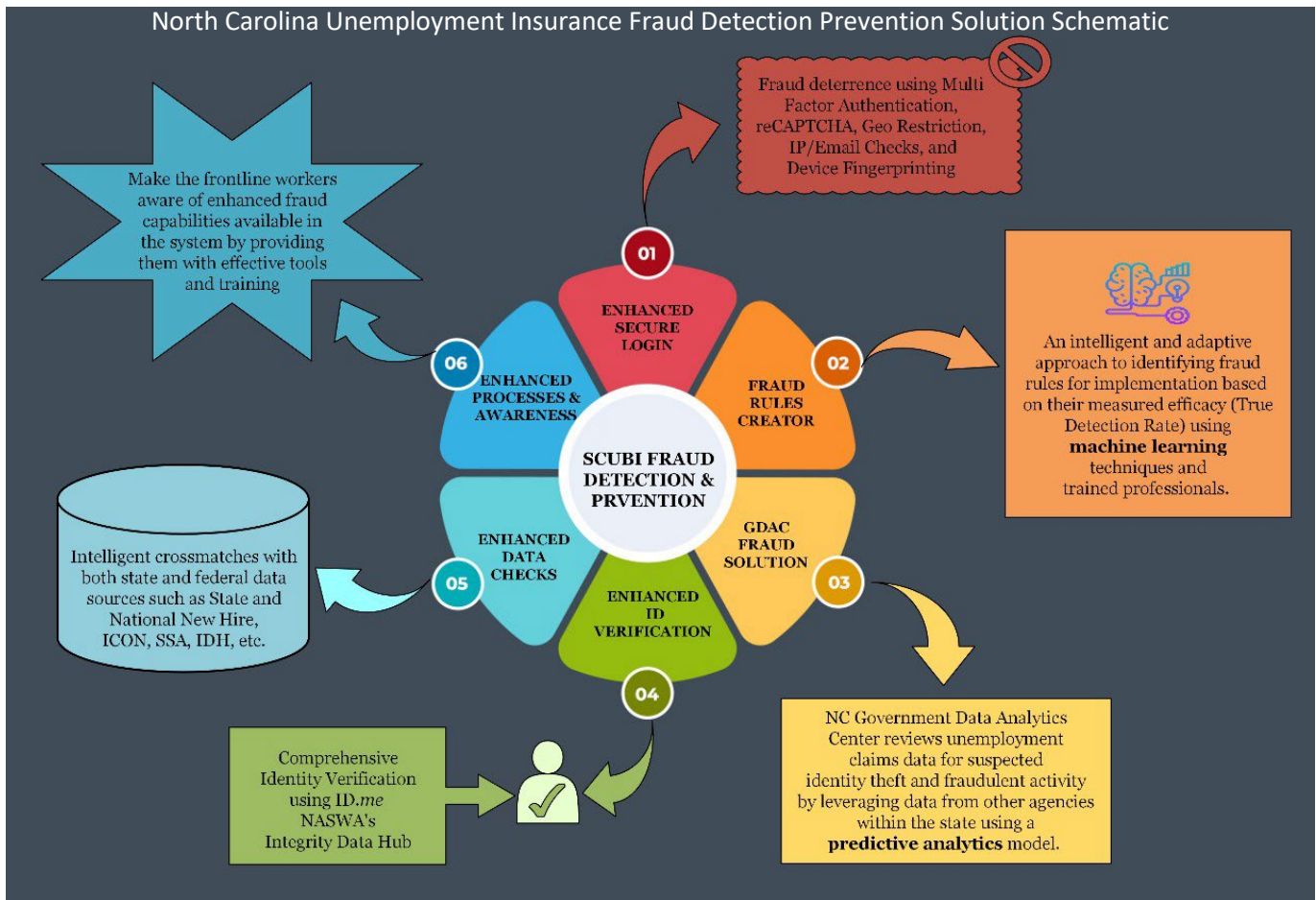
1. Enhanced Secure Login

The following checks were added into the claimant login process:
- o reCAPTCHA at initial login.
- o Intelligent Multi Factor Authentication.
- o Collection and analysis of device fingerprinting data.
- o Restrictions to site access based on geolocation.
- o Verification of IP and email addresses against suspicious lists.

2. DES Fraud Rules Creator

The DES Fraud Rules Creator was developed using artificial intelligence and machine learning to create fraud rules that indicate suspicious activity on a claim for unemployment benefits. The process is continuously evolving using Lasso and Support Vector Machine feature selection methods to identify new rules to adapt to the dynamic nature of fraudulent behavior. DES has a dedicated team and a process to test and measure efficacy of the proposed rules by calculating their respective True Detection Rates (TDR). The TDR assesses rules individually or in combination when applied against a subset of claimant data and is calculated as the percentage of claimants in the set who did not pass or complete the required identity verification checks.

Through this process, it was determined there is a higher chance of potential fraud if the claim is a match on multiple rules. It was also found that after implementing machine learning classification methods, specific combinations have drastically higher rates of identifying identity theft. This allowed us to focus our investigation efforts on the high-risk claimants and not burden the low-risk ones. To date, we have implemented 102 rule checks in the production environment and continue to analyze others. GDAC performs the rule checking, which is explained in detail in the next section.
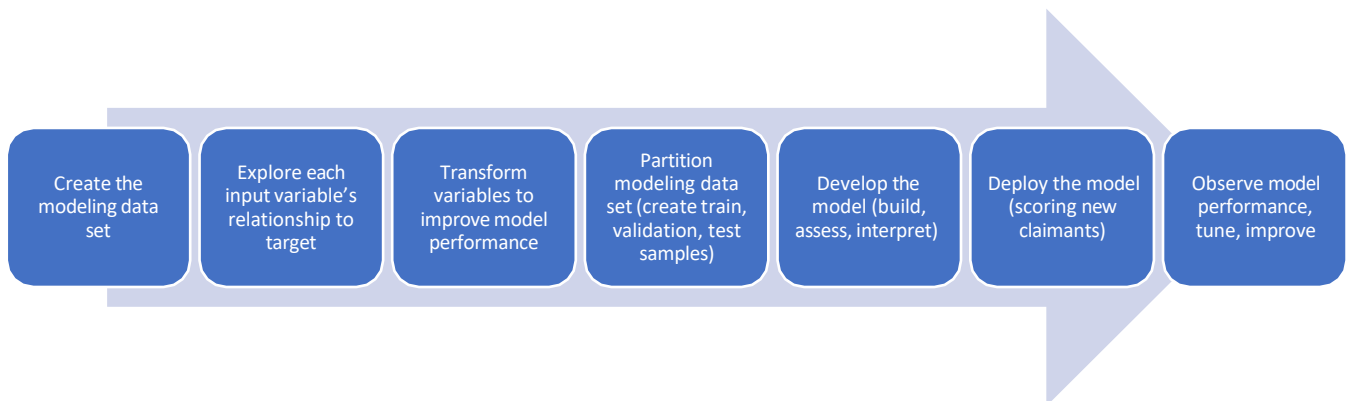
The rules are used to help DES decide which claimants should be subject to additional ID verification checks. The easiest option would be to subject every user to these checks; however, that is neither practical nor sustainable for the following reasons: a) delays in processing the claim could be significant during the high-volume periods, b) added inconvenience and fatigue for a majority of otherwise legitimate claimants, and c) added transactional costs. Therefore, the best solution is to route specific users for added ID verification based on a well-defined fraud score threshold.

The flagging of suspicious claims for additional ID verification occurs at two stages: first, when a user successfully registers in the benefits system, and then when they submit their claim for unemployment benefits. The system checks the registration data against a set of rules/heuristics and flags suspicious accounts. Flagged users will then be routed to an external service provider, ID.*me*., for identity verification. The second stage uses the claim submission data to flag suspicious claims. The multi-stage approach helps deter fraud early in the process, reducing the number of fraudulent claim submissions.

3. GDAC Fraud and Identity Theft Solution

DES partnered with the N.C. Government Data Analytics Center to develop the GDAC Fraud Solution **predictive data analytics models** to review unemployment claims data for suspected fraudulent activity by leveraging data collected from other North Carolina state agencies.

Based on top suspicious combination pattern factors identified during claim submission, predictive models assign a probability and **score** to an individual's fraud potential. The higher the score, the higher chance that the claim is fraudulent. The current model uses a random forest classifier. The high-level modeling development and deployment process is as shown below:

| Create the modeling data set | Explore each input variable's relationship to target | Transform variables to improve model performance | Partition modeling data set (create train, validation, test samples) | Develop the model (build, assess, interpret) | Deploy the model (scoring new claimants) | Observe model performance, tune, improve |

The GDAC Fraud and Identity Theft Solution suite consists of the following features:
  o Integrated claims data with other data available to the state to surface anomalies that may indicate a suspicious identity-related fraud.

- o Executive dashboard that aggregates the claims benefit GDAC alerts and associated outcomes.
- o Automatic integration of alerts into SCUBI for immediate and preventive action as identified by DES fraud investigators.
- o Enhanced existing work and earnings, new hire, deceased and incarceration alerts to identify additional fraud in pandemic unemployment assistance claimants.
- o Retroactive analysis of deceased and incarcerated claimants.

The Benefits Integrity Alert (BIA) Visualization Tool supports:
- o Identification of suspected claimants by clustering claimants across similar suspicious characteristics using DES and other state agency data.
- o Displaying suspicious claimants using an intuitive heat map for a streamlined investigation process and immediate action.
- o Providing a self-service lookup interface for investigators to make filtered searches.

The Alert Cluster Summary Map gives the DES investigator a geographical view of the alerts and visual information on the ranking of the alert.

The color of the bubble is driven by the cluster ranking assigned to each alert:

- o Ranks of 95 and above are RED
- o Ranks between 95 and 80 (inclusive) are YELLOW
- o Ranks below 80 are GREEN

Once generated, the predictive model and business rule alert results are automatically integrated into the SCUBI benefits system for timely investigation and action based on the findings.

4. Enhanced Identity Verification

As part of its fraud prevention efforts, DES has partnered with two different third parties for enhanced identity verification services, ID.*me* and the National Association of State Workforce Agencies' Identify Verification (IDV) service.

To prevent and detect potential identity theft, the ID.me service validates and verifies the legitimacy of claimants to ensure they are who they say they are when applying for unemployment benefits. This process also serves as a 'speed bump' to fraudsters trying to submit claims with stolen claimant credentials in mass scale across multiple states. Many fraudsters do not further pursue the claim submission process once they approach this step; therefore, it serves as an effective deterrent. Over 95% of the claimants verified through this service are processed automatically. The remaining 3 to 5% require manual interventions (i.e., trusted referee process with an ID.me representative) for further ID verification. DES's fraud solution provides flexibility in relation to identity verification, in that it is not tied to any particular third-party identity verification provider, and we can control which claimants will be subject to this process based on a well- defined fraud score threshold.

Identity Verification service (IDV) is a newly offered automated service from the National Association of State Workforce Agencies' Integrity Data Hub (IDH). The IDH provides critical unemployment benefits data crossmatching across states to combat fraud. Powered by the Experian Precise ID solution, this powerful tool provides centralized ID verification for all claims in participating states. The resulting data may overlap with what is known from ID.me, but it provides an additional level of protection to identify indicators of potential fraud. As IDV continues to mature, DES may rely more on this service in the future.

Currently, DES submits a subset of its claim and claimant population data to the IDH based on certain criteria but will soon send all new claims data to the hub and update the SCUBI benefits system database with the responses

received. The response data includes some valuable information, such as synthetic ID flag, fraud scoring and the associated reason codes for further investigation by the DES fraud team. There are many more data crossmatch checks done through IDH that are explained in the Enhanced Data Checks section below.

5. Enhanced Data Checks

DES has integrated multi-faceted data crossmatching and validation services between the SCUBI benefits system and various third-party service providers, including GDAC, Optimal IdM identity management services, the National Association of State Workforce Agencies Integrity Data Hub, ID.*me*, the state and national Directories of New Hires, the Social Security Administration, and others. SCUBI implemented some of these interfaces/interactions as microservices that are deployed on Amazon Fargate instance as a docker image and live separately from the core SCUBI application.

In addition to the many traditional cross matching services (National Directory of New Hires, Social Security Administration, etc.) that were in place, the following new services were implemented during the pandemic:

Enhanced National Association of State Workforce Agencies Integrity Data Hub (IDH) Checks
- o Added IDH interface for Identity Verification (IDV).
- o Established channel and process to report suspicious claimant attributes to NASWA's Suspicious Actor Repository (SAR).
- o Implemented multistate SAR crossmatch to find suspicious actors reported by other states.
- o Implemented Foreign IP address detection and suspicious email domain checks.
- o Established Fraud Alerting channel – a secure space for states to collaborate regarding existing and emerging fraud schemes observed.
- o In the process of implementing Banking Account Verification checks.

State Directory of New Hires (SDNH)
- o Added SDNH crossmatch service on the weekly certification process to create investigations for the claimants detected with reported earnings and new hire information.

SIDI -IBIQ (State Identification Inquiry – Interstate Benefit Inquiry System)
- o Added additional SIDI-IBIQ real-time service on weekly certification process to identify claimants with out of state wages, claims and/or potential eligibility in another state.

6. Enhanced Processes and Awareness

While new technologies provide excellent tools for fighting unemployment benefits fraud, people play a crucial role in using these tools effectively and acting on the data to make sound, timely decisions. The following are some of the measures DES has taken to reinforce its effectiveness in using our fraud prevention solutions.

- o Engaged McKinsey consulting services to help set up required fraud processes, dedicated team structures, awareness campaigns and training.
- o The McKinsey team trained the DES core senior team on the Ability to Execute Essentials. This curriculum provided enterprise-wide solutions on the skills and mindsets that matter most to unlock an organization's full potential, while empowering employees to improve the way they work. The DES internal team later rolled this training out to the rest of the organization to help manage workloads more efficiently.
- o Began implementing the use of digital dashboards for making data-based operational decisions. Newly implemented dashboards helped the agency spot anomalies, resulting in timely and appropriate remedial action.
- o The DES fraud team created a data-driven unemployment fraud process that automates the detection of fraudulent activity. This process defines parameters for detection and proposes statistical and Machine Learning methods the team can use to automate solutions for new suspicious behavior.
- o Established a dedicated Fraud Hotline and created intelligent online webforms for the public to report fraud and ID theft. The resulting leads were investigated by our well-trained Benefits Integrity team.

IMPACT

Preventing fraud, waste, and abuse in the unemployment benefits system has long been a priority for the N.C. Division of Employment Security and, at the federal level, the U.S. Department of Labor. It became an even more pressing issue during the COVID-19 pandemic among reports of new and more sophisticated fraud threats. In particular, schemes involving fraudsters using people's stolen identifying information to claim unemployment benefits became widespread across the country.

These fraud schemes victimize innocent people, negatively impact the employers who pay taxes into the unemployment system and put a strain on limited public resources.

Responding to the urgent need during the pandemic, DES successfully implemented a multi-layered technology solution that uses data analytics and visualizations to prevent and detect fraudulent activity. This has provided DES with the ability to stop fraudulent claims with a higher degree of accuracy early in the process, ideally before any benefits are paid. With an over 660% increase in total claim volume, it was critical that DES find new ways to determine whether submitted claims were fraudulent. The automation tools incorporated into the fraud detection solution helped DES focus attention quickly, be more responsive, and ensure that benefits were paid to those who needed the money. By stopping payments before they go out rather than trying to collect once they've been paid, DES's fraud detection solution significantly reduces burden on the back end of process.

Additionally, DES has made significant improvements to its processes and the effective use of fraud tools among our staff.

In 2021, DES's fraud solution yielded the following results:
- o The implementation of 102 (and counting) fraud rule checks in the production environment since the pandemic started.
- o Predictive model rules with a True Detection Rate of 75%. This means three quarters of claimants suspected of fraud did not complete or pass the additional verification checks required by DES.
- o 281,665 potential claimant misrepresentation/fraud issues were identified. DES presumes 147,405 of those to be fraudulent due to confirmed fraud or a claimant's failure to report to DES.
- o Using a simplified estimate of an average $5,178 paid per claim in 2021, we can extrapolate that $264 million in fraudulent payments were prevented based on 50,966 denied claims due to misrepresentation.
- o Information about 161,000 suspicious individuals was sent to the NASWA national Suspicious Actors Repository to share with other states to prevent multi-state fraud schemes.
- o The process helps DES focus on claims with a high probability of fraud, so the majority of legitimate claimants are not burdened with additional verification checks.

In conclusion, DES has implemented an innovative fraud detection and prevention solution, mature processes, a well-trained workforce, and enhanced capabilities to combat unemployment benefits fraud. Partnerships with entities like GDAC helped break down barriers of siloed data, allowing us to protect constituent data and provide services in ways that were not previously possible. We continue to invest in the areas of fraud prevention, digital dashboards, and real-time integration initiatives for further refinement in 2022 and beyond.

DES also believes its fraud solution can serve as a model that other states can adapt and adopt to meet their needs. The solution is implemented such that it constantly improves on itself using new data sources and adaptive analytic techniques in the face of varying fraudulent behavior. The first potential state to benefit is South Carolina, which shares an unemployment benefits system with North Carolina that is managed by the same vendor.

With these multi-layered solutions and lessons learned during the COVID-19 pandemic, North Carolina and states across the country can be better prepared to fight unemployment fraud in future economic downturns, natural disasters or emergency events.