FORVIS

FRAUD INVESTIGATION SERVICES REPORT FOR UNEMPLOYMENT COMPENSATION MODERNIZATION AND IMPROVEMENT COUNCIL ON BEHALF OF THE KANSAS LEGISLATURE ("COUNCIL")

SEPTEMBER 1, 2022

Version 6.22

FORVIS

130 E. Randolph Street, Suite 1900 / Chicago, IL 60601
P 312.288.4653 / **F** 312.288.4672
forvis.com

September 1, 2022

Sean Tarwater, Chairperson
Unemployment Compensation Modernization and Improvement Council
300 SW. 10th Ave., Ste. 551
Topeka, KS 66612

Dear Mr. Tarwater:

Thank you for the opportunity to provide investigation services for the Unemployment Modernization and Improvement Council (the Council) in connection with the effects on the Kansas Department of Labor (KDOL) and the unemployment insurance system of fraudulent claims and improper payments during the period of March 15, 2020, through March 31, 2022. For our analysis, we relied upon information provided to us in the form of electronic unemployment insurance claims files, documents, as well as conversations and interviews with relevant parties. This report is based on work completed to date.

Our services were provided in accordance with the Statement on Standards for Forensics Services promulgated by the American Institute of Certified Public Accountants and, accordingly, do not constitute a rendering by **FORVIS, LLP** (FORVIS) or its partners or staff of any legal advice, nor do they include the compilation, review, or audit of financial statements. Because our services were limited in nature and scope, they cannot be relied upon to discover all documents and other information or provide all analyses that may be of importance in this matter. We were asked to analyze certain designated files, data, and information and, based on the scope of work, we identified matters discussed in this report, including an estimate of potential fraudulent payments based on data analytics procedures. This is a factual report of our findings, and we do not make a determination on if specific claims are fraudulent or comment on legal culpability.

This report is the property of FORVIS and has been prepared solely for use by the Council and should not be used by any other party or for any other purpose, without our written permission in each specific instance.

The validity of this report is predicated on the extent to which full, honest, and complete disclosure was made by all parties. We reserve the right to supplement this report if additional information becomes available.

FORVIS, LLP

FORVIS, LLP

Robert R. Sprague

Robert R. Sprague, CPA

Table of Contents

Overview of Project and Data

During the COVID-19 pandemic, additional federal funding and flexibility were provided to state unemployment insurance agencies to help address the increase in unemployment insurance claims. These state unemployment insurance agencies became a target for potential fraud, and the Kansas Department of Labor (KDOL) was no exception. We have been asked to gain an understanding of the effects of these potentially fraudulent claims on KDOL's unemployment insurance system as well as KDOL's response during the period March 15, 2020[1] through March 31, 2022 (the "Period"). A complete listing of the Scope of Work can be found in Attachment A of this document. The items covering KDOL's information technology security included in the scope of services were previously covered by FORVIS in two reports issued to the Council on May 11, 2022.

We received data from KDOL representing 1,540,957 million claims representing 1,086,195 million unique claimants, and payments totaling $3,554,882,327 for the Period. Our understanding is that the Lost Wages Assistance program is out of scope for purposes of this report, as that is not an unemployment insurance program. As such, we have excluded those payments, which total $130,565,088, from our analysis. As further described below, our data analysis indicates an estimated range of between approximately $441 and $466 million potentially fraudulent claims were paid during the Period[2].

Self-Reported Fraud

We received 329,553 records of data representing claimants who had self-reported a fraudulent claim, or had someone, such as their employer, report fraud on their behalf. KDOL collected this data from the online Kansas unemployment insurance fraud reporting tool at https://reportfraud.ks.gov/.

KDOL Potential Fraud Flag

KDOL flags claimants as potentially fraudulent for several reasons, such as if a claimant self-reported fraud or if that claimant used the same bank account as a significant number of other claimants. While there were many different reasons why KDOL flagged a claimant as potentially fraudulent, the reasons why specific claimants were flagged as potentially fraudulent were not tracked consistently. We received two files that contained, in addition to other information, information regarding which claimants had been flagged by KDOL as potential fraudulent claimants, but not the specific reason why the claimant had been flagged. Between these two files, 350,137 claimants were flagged as potential fraud and had not been subsequently cleared as legitimate.

IP Addresses

Each time a claimant logs into the KDOL system, their IP address is recorded. We obtained a data set of 24,664,279 logins that provided the IP addresses for claimants that filed online claims.

Deceased Claimants

KDOL provided a listing of deceased claimants which provided date of death for 8,901 claimants.

Incarceration Records

KDOL provided a listing of 70,468 records identifying claimants who had been incarcerated at some point in time according to data KDOL had matched against Kansas Department of Corrections data. This data included claimants with claims in our scope period, but also claimants outside of our scope period. We noted many claimants appeared in this data multiple times with the same incarceration date. We considered this duplication in our analysis.

[1] The scope period outlined in the Agreement for Fraud Investigations Services was March 15, 2020 to March 31, 2022; however, FORVIS received unemployment insurance claim and payment data from January 1, 2020, to March 31, 2022.

[2] Our initial estimate of potentially fraudulent claims was between approximately $486 million and $511 million. As further described below, we have reduced this estimate to account for the possibility that legitimate claims were filed at a later date by claimants that were the victim of an earlier fraudulent claim filing using their stolen personal information.

Summary Claim Information by Employer

KDOL provided a summary of claims by employer, program, month, and year for January 2015 through March 2022, containing 1,320,176 records. In addition, KDOL provided a summary of payments by employer, program, month, and year for January 2015 through March 2022, containing 1,295,415 records.

Self-Reported Fraud Analysis

We utilized the self-reported data from the online Kansas unemployment insurance fraud reporting tool at https://reportfraud.ks.gov/ to identify claimants who had self-reported a fraudulent claim, or had someone, such as their employer, report fraud on their behalf. This data did not contain a claimant ID to enable us to link directly with the claimant data we had been provided, but did include names, some full SSNs, some partial SSNs, and birth dates. We used various combinations of these data elements to match the data between these disparate data sets. After accounting for duplicate reports for the same claimant, we were able to match this self-reported fraud claimant database with 227,918 claimants in the claims database. Of these 227,918 claimants, 115,812 had received payments, totaling $282,469,430. The average total payments to claimants who had self-reported fraud was $2,439.

Overview of Data Analytics Methodology

We used the self-reported fraud claims as our starting point for assessing potentially fraudulent claims and then built additional detection methods on top of that to increase the probability of identifying potential fraud. We employed the following three additional methods:

- Egregious Flag Method
- Machine Learning Method
- Cumulative Risk Score Method

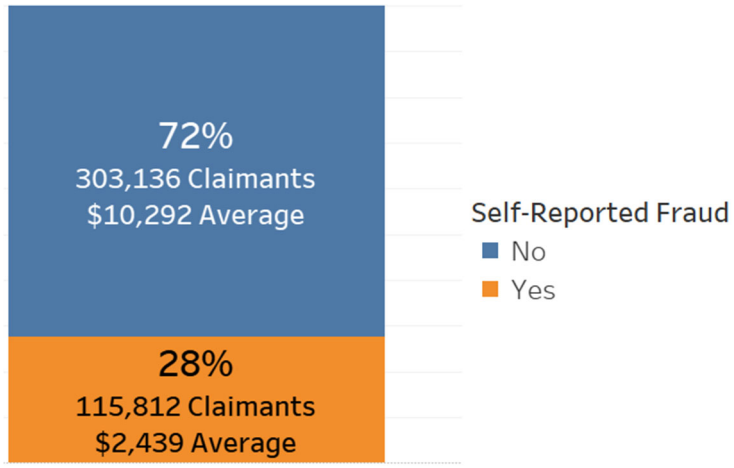
All three of these methods were based on a series of potential fraud flags, such as ***claimant shares a bank account with other claimants*** or ***claimant with a high email address risk score***. The egregious flag method identified specific potential fraud flags that, by themselves, appeared to indicate a high probability that the claim was fraudulent.[3] The machine learning method identified claimants with combinations of potential fraud flags that were consistent with those associated with self-reported fraud claims. The cumulative risk score method assigned a value to each potential fraud flag, summed those scores, and assigned a total risk score to each claimant.

To inform these methods, we started by studying the population of claimants who had received at least one payment, split between claimants with self-reported fraud and those without. By doing so, we learned two key pieces of information we used throughout our analysis.

First, we learned that claimants with self-reported fraud made up **28%** of the population of claimants with payments. This was a helpful baseline in our assessment of the efficacy of various procedures we performed, as well as in our assessment of the efficacy of KDOL's potential fraud flags.

Second, we learned that the average of payments to claimants with self-reported fraud, **$2,439**, was considerably lower than the average to claimants without self-reported fraud, **$10,292**. Intuitively, this makes sense given our understanding from discussions with KDOL that the Department was considering all information that was available regarding potential fraudulent claimants and stopping payments when they became aware of a potentially fraudulent claimant. Therefore, a claimant may have started to receive payments but been stopped midway through the expected payment stream.

Figure 1 – All Paid Claimants



[3] As further described below, our analysis determined that 66% to 70% of the claimants that were flagged by an egregious procedure also had self-reported fraud, suggesting a strong correlation between the egregious flags and claimants with self-reported fraud.

Potential Fraud Flags

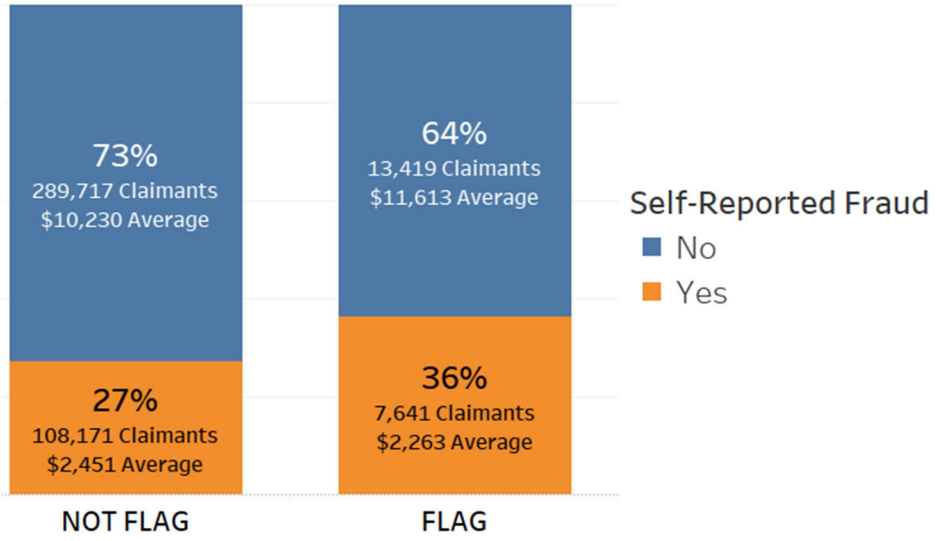
We utilized 53 potential fraud flags in our analyses. We assigned a risk score to each flag, based on how predictive the flag appeared to be. Flags with no predictive capacity were assigned a score of zero, and flags with the highest predictive capacity were assigned a score of 10.

Scoring for Single Value Flags

For flags that were binary, meaning either the claimant was flagged by the test or not, a single score was assigned. To assess a test's predictive value, we compared the percentage of claimants with self-reported fraud who did NOT get flagged relative to the percentage of claimants with self-reported fraud who did get flagged. As an example, the below potential fraud flag identified claimants whose personal address matched the employer address listed on their claim. In figure 2 below, we can see in the left bar that for those claimants not flagged, approximately 27% had self-reported fraud. In the right bar we can see that for those flagged, approximately 36% had self-reported fraud. So, the test appeared to have some predictive value because the percentage of claimants in the subset of claimants flagged (the right bar) was higher than those not flagged (the left bar).

For this test, we assigned a score of two. For reasons explained later in the report, we determined the score using a scale that ranged from 28% of claimants with self-reported fraud for tests with no predictive capacity, since that is our baseline across all claimants, to 66% for tests with the highest predictive capacity, since that is the highest threshold achieved in the egregious section of the report. A score of zero was assigned if the flag resulted in 28% or 10 if the flag resulted in 66%.

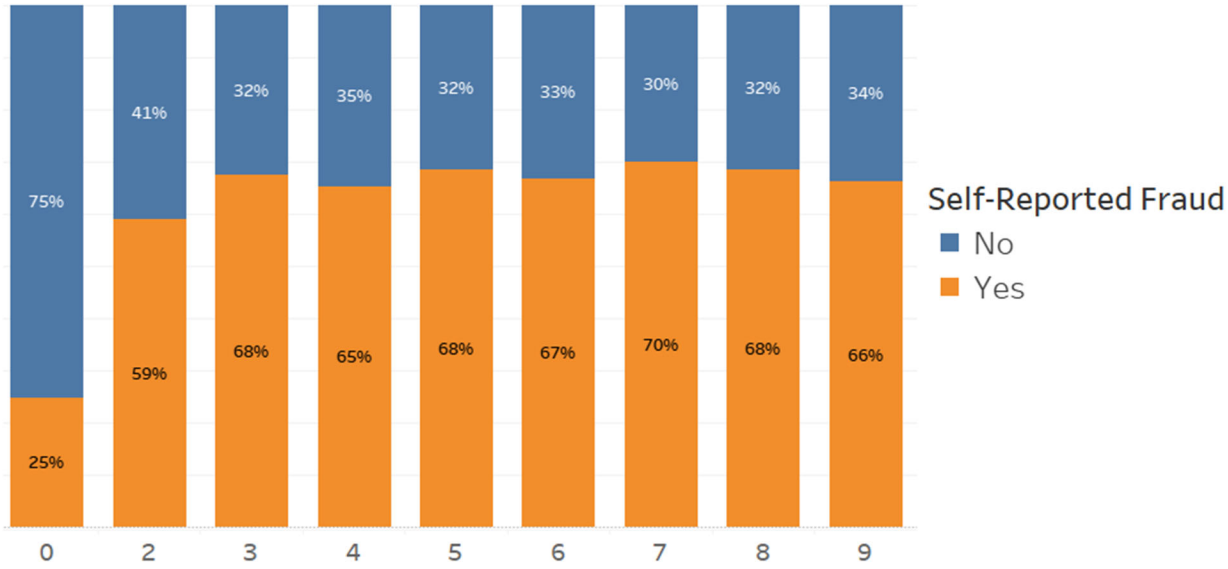
Figure 2



Scoring for Multiple Value Flags

For flags with multiple potential values (three claimants sharing an attribute, four claimants, five claimants etc.), we considered not only whether the claimant was flagged but also the value associated with the flag. As an example, one of the flags we created was to isolate email addresses which differed only by special characters, such as periods (for example, A.c.me@gmail.com, Ac.m.e@gmail.com, and A.c.m.e@gmail.com). If a claimant shared a similar email address with multiple other claimants, we assigned a score based on the number of claimants with that shared similar email address. In Figure 3 below, which represents the results of claimants who share a similar email address, the second bar represents claimants who share a similar email address with one other claimant or, said another way, a shared similar email address between two claimants. Within this subset of claimants, 59% had self-reported fraud, and a score of eight was assigned. For claimants in the rightmost bar, emails shared across nine claimants, 66% had self-reported fraud, and a score of 10 was assigned.

Figure 3



We noted that as the number of similar emails increased, illustrated by moving left to right in Figure 3 above, initially the percentages for self-reported fraud increased dramatically, and then seemed to level off around 66%. This led us to consider the fact that at a certain point, perhaps claimants at or above the threshold where it levels off could be potentially fraudulent. However, we analyzed additional data to support this hypothesis.

Egregious Flag Method

The goal of the egregious flag method was to identify specific potential fraud flags that, individually, appeared to flag claims with a high probability of potential fraud. We had two requirements for a flag to be considered an egregious flag:

- First, it had to intuitively make sense to be egregious. As an example, if three claimants had similar email addresses that differed only by special characters (for example, A.c.me@gmail.com, Ac.m.e@gmail.com and A.c.m.e@gmail.com), it seems likely that those three claimants would be potentially fraudulent.
- Second, the data had to support the decision. The following explains how we used the data available to us to determine whether to consider a potential fraud flag to be egregious.

We identified two subsets of claimants that we believed a reasonable person would agree would have a high probability of being potentially fraudulent, based on three unique combinations of potential fraud flags.

Egregious Claimant Subset #1

The first subset of claimants exhibited all three of the following attributes:

1) Claimant shared a bank account with nine or more other claimants
2) Claimant shared an email address with nine or more other claimants
3) Claimant had a vendor-defined IP address potential fraud score of at least a nine out of 10

This subset consisted of 599 claimants:

- 66% of these claimants had self-reported fraud, and the average claimant payments were $1,666.
- 34% of these claimants had NOT self-reported fraud, and the average claimant payments were $2,835.

Egregious Claimant Subset #2

The second subset of claimants exhibited all three of the following attributes:

1) Claimant shared a phone number with nine or more other claimants
2) Claimant shared an email address (excluding special characters) with nine or more other claimants
3) Claimant had a vendor-defined email potential fraud score of at least a nine out of 10

This subset consisted of 730 claimants:

- 70% of these claimants had self-reported fraud, and the average claimant payments were $1,511.
- 30% of these claimants had NOT self-reported fraud, and the average claimant payments were $2,449.

For these subsets, which we believe a reasonable person would agree have a high probability of being potentially fraudulent, 66% and 70%, respectively, of claimants had self-reported as fraudulent. This means between 30% and 34% of these claimants had a high probability of being potentially fraudulent but did NOT self-report as fraud.

Egregious Flag

We noted roughly the same percentage of claimants with self-reported fraud across these four subsets of claimants:

- 66% in the egregious claimant subset #1,
- 70% in the egregious claimant subset #2,
- 69% in the subset of claimants where three or more claimants shared an email address, after removal of special characters, and
- 67% in the subset of claimants where three or more claimants shared a bank account.

Based on this analysis, we believed it was reasonable to assume that, if an individual potential fraud flag isolated a subset of claimants where between 66% and 70% of those claimants had self-reported fraud and it intuitively made sense to consider the potential fraud flag as egregious, then there was a high probability that the claimants flagged by that test were potentially fraudulent.

Using this methodology, we identified two potential fraud flags which we considered to be egregious.

1) Three or more claimants with the same email address, after removal of special characters (for example, A.c.me@gmail.com, Ac.m.e@gmail.com, and A.c.m.e@gmail.com), which resulted in a subset of paid claimants whereby 69% of those paid claimants had self-reported fraud
2) Three or more claimants with the same shared bank account, which resulted in a subset of paid claimants whereby 67% of those paid claimants had self-reported fraud

We further considered whether a specific potential fraud flag was egregious purely based on the nature of the test, and identified one paid claimant with an invalid SSN, and nine paid claimants with a death date prior to their claim dates which we flagged as egregious.

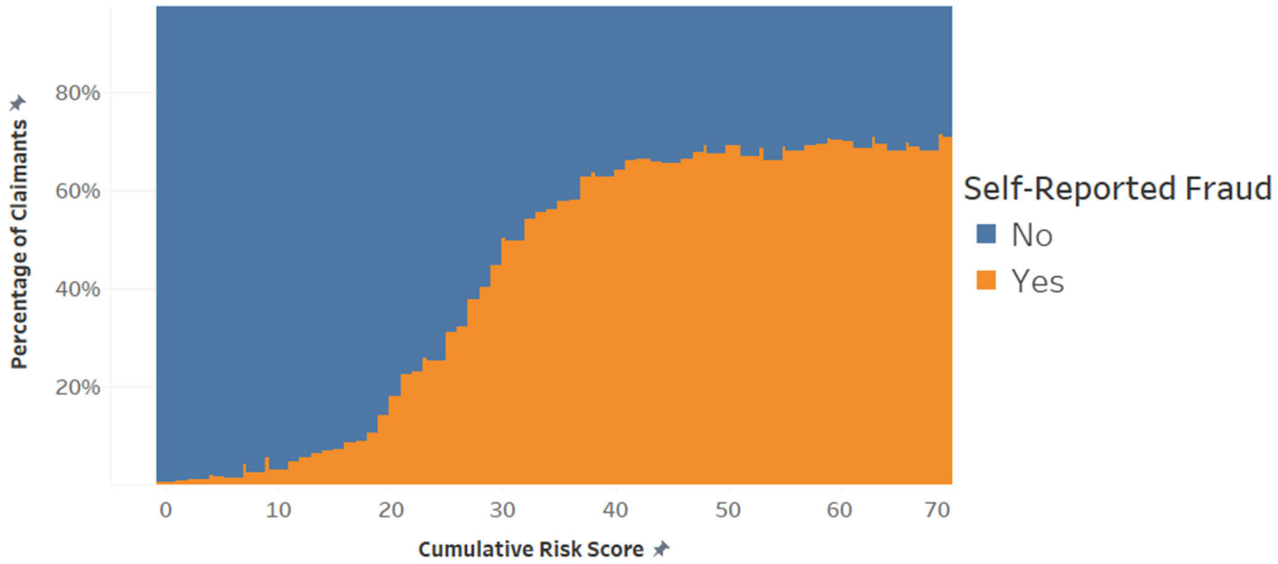
Machine Learning Method

While the egregious flag method was focused on finding a single potential fraud flag that was very predictive of fraud by itself, the machine learning approach was focused on finding unique combinations of potential fraud flags with high predictive value. We trained the model by showing it claimants that had self-reported fraud as well as those that did not have self-reported fraud and asking the model to try to find combinations of flags within the self-reported fraud population that also existed in the population without the self-reported flag.

Cumulative Risk-Score Method

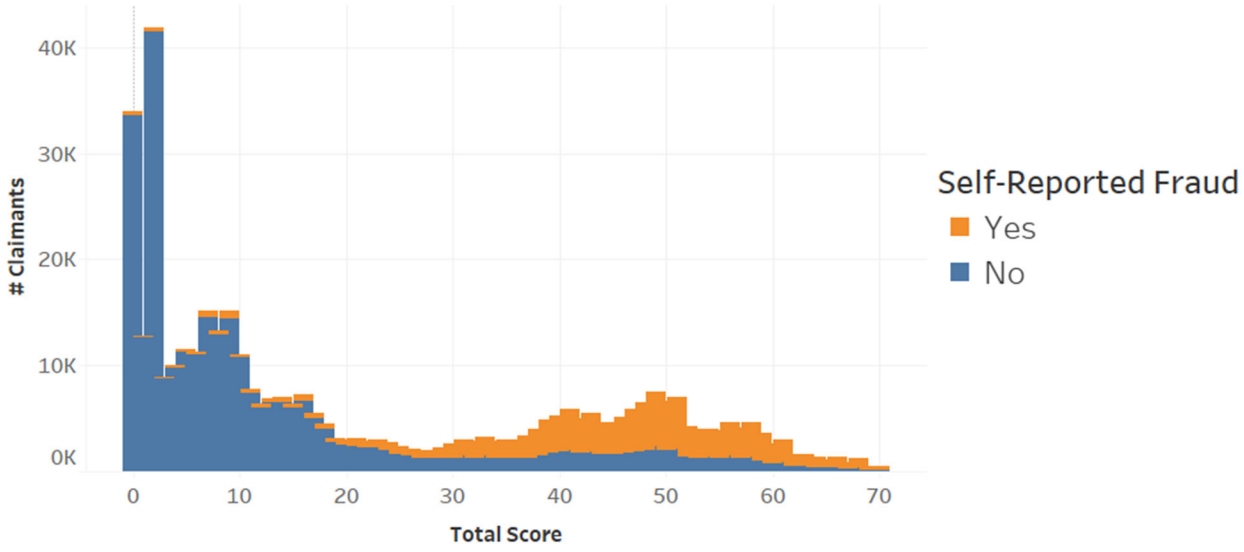
The cumulative risk-score method simply summed up the scores from the potential fraud flags associated with a claimant. Claimants over a certain threshold were determined to be potentially fraudulent. We judgmentally selected a threshold of 40, based on a data-driven approach. First, we noted the average cumulative risk-score for claimants with self-reported fraud was 40. Second, we used data visualization software to help us better understand the distribution of claimants across the various risk score thresholds, focusing once again on the percentage of self-reported fraud claimants relative to the other claimants initially. In Figure 4 below, orange represents claimants with self-reported fraud, and blue represents claimants who did not self-report fraud. On the leftmost side, at a risk score of zero, there is a very small orange bar which indicates approximately 1% of claimants with a risk score of zero had self-reported fraud. On the rightmost side, at a risk score of 70, there is a very large orange bar which indicates approximately 71% of claimants with a risk score of 70 had self-reported fraud. This distribution levels off at a risk-score of approximately 40.

Figure 4



While Figure 4 above shows the percentage breakdown of claimants at each risk score, Figure 5 below shows the breakdown of the number of claimants at each risk score, which provides helpful context.

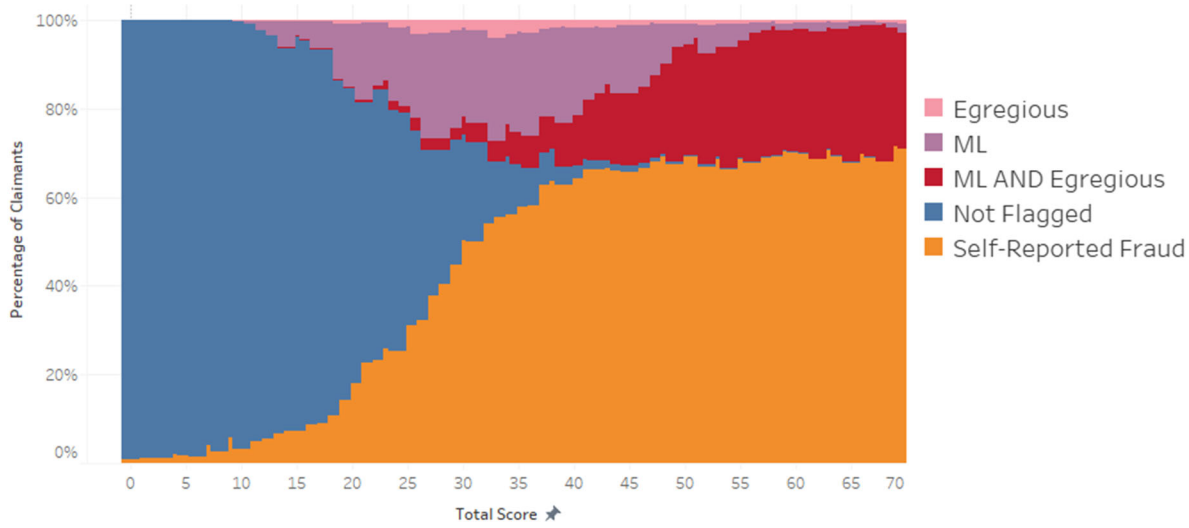
Figure 5



Combination of All Methods

Starting with the self-reported fraud claimants as our baseline in Figure 4 above, we then layered in the claimants flagged by our egregious flag and machine learning methods. These independent methods produced very similar results in the higher cumulative risk score levels, as shown in red below, and while there was overlap between these two methods in the lower cumulative risk scores, there were also some claimants flagged by one method and not the other, which is expected since one identifies a single flag which is consistent with potential fraud, and the other identifies combinations of flags consistent with potential fraud.

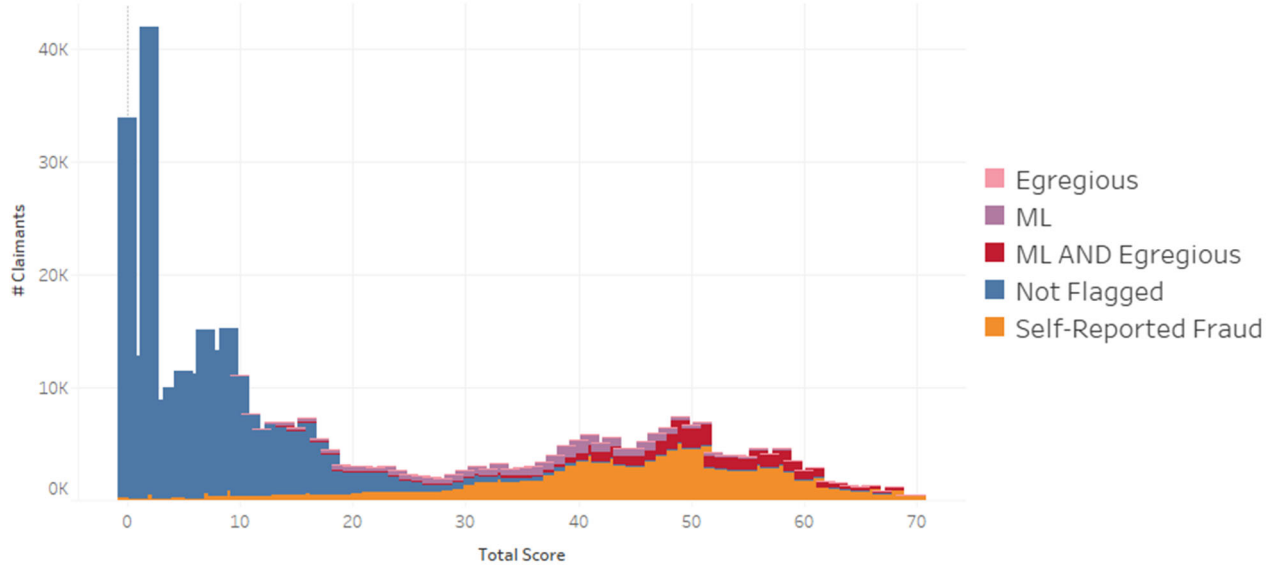
Figure 6



The secondary feature of Figure 6 above is that it further supports our earlier conclusion that a cumulative risk score of 40 is appropriate as a cutoff for our cumulative risk score method, as there are very few claimants not already flagged as potentially fraudulent at a score of 40 or above, as shown by the blue area in the graphic above.

While Figure 6 above shows the percentage breakdown of claimants at each risk score, Figure 7 below shows the breakdown of the number of claimants at each risk score, which provides helpful context.

Figure 7



Taking these approaches together, including the self-reported fraud flag, we have estimated the total payments to potentially fraudulent claimants to be between $486 million and $511 million. The low end of the range includes claimants with self-reported fraud and/or claimants identified by our machine learning method. The high end of the range includes these same claimants plus claimants flagged by the egregious flag method and/or the cumulative risk-scoring method and is the figure we will use throughout the remainder of this report. We noted the average cumulative risk score for potentially fraudulent claimants not self-reported as fraud was 39, which is consistent with the average risk score for claimants with self-reported fraud of 40. The average of total payments to potentially fraudulent claimants who had not self-reported fraud was $4,057, which is slightly higher than the average of claimants with self-reported fraud of $2,439. This aligns with expectations, as we understand that KDOL was stopping payments to self-reported fraud claimants as well as claimants that had other patterns consistent with fraud, so we would expect the average of payments to claimants who did not have a self-reported fraud to be higher, resulting in an overall higher average.

Of the $511 million potentially fraudulent payments, approximately $310 million related to state programs, and $201 million related to federal programs.

Of the $511 million potentially fraudulent payments, approximately $436 million was paid before the implementation of the multifactor authentication requirement implemented by KDOL, and approximately $75 million was paid after.

Of the claimants identified as potentially fraudulent, approximately 98.5% filed their claim(s) via the internet, and approximately 1.5% filed their claim(s) by phone. Of the claimants not identified as potentially fraudulent, approximately 81.7% filed their claim(s) via the internet, and approximately 18.3% filed their claim(s) by phone.

Of the $511 million potentially fraudulent payments, approximately 87.4% were paid by direct deposit, and approximately 12.6% were paid by prepaid debit card. Of the payments not identified as potentially fraudulent, 75.3% were paid by direct deposit, and approximately 24.7% were paid by prepaid debit card.

Legitimate Claims Following Potentially Fraudulent Claims

Our analysis utilized individual claim level detail for purposes of flagging potentially fraudulent claims, but, ultimately, a claimant was determined to be potentially fraudulent or not. KDOL raised concerns that this would tend to overstate the potential fraud because there were instances where legitimate claimants filed for unemployment only to discover that a fraudulent claim had previously been filed utilizing their personal information. Therefore, our analysis would categorize all payments to this claimant as potentially fraudulent when only a portion should be categorized as potentially fraudulent. While it is not possible to determine an exact dollar amount that follows this pattern since we do not have the self-reported date for all potentially fraudulent claims and we cannot say definitively that all new claims paid after a self-report were legitimate, we have developed an approach to provide some insight into the magnitude of this situation.

For self-reported fraud, we have the date of the reported fraudulent claim. If a claimant with self-reported fraud subsequently filed a claim and you assume that claim was legitimate, then any subsequent payments would presumably be legitimate as well. The total of such payments was approximately $25 million.

We previously calculated payments to claimants who had self-reported fraud to be $282 million, which represents 55% of the total payments to potentially fraudulent claimants of $511 million. If we assume the same proportion of payments for legitimate claims in the population of self-reported fraud claimants to the total population of potentially fraudulent claimants, we can estimate that $45 million ($25 million/55%) of the total $511 million could have potentially been for legitimate claims following fraudulent claims. If these payments were legitimate, that would reduce our estimated potential fraudulent claim range to between $441 and $466 million.

Evaluating the Effectiveness of KDOL Fraud Flags

As described in the Overview of Data section of this report, we received a file which identified 350,137 claimants as having been flagged as potentially fraudulent by KDOL. When we isolate to claimants flagged by both FORVIS and KDOL, there is an overlap of $382 million of payments.

In addition to flagging $382 million of claims which were also flagged in our analysis, the KDOL flag identified an additional $345 million of payments as potentially fraudulent. The average cumulative risk score for this subset of claimants was 19, which is considerably below the average of 40 we noted for claimants with self-reported fraud. The average total payments to claimants in this subset was $12,084, which is well above the average of claimants with self-reported fraud of $2,439. Taking these two pieces of information together, it appears many of these claimants were likely legitimate and should not have been flagged.

Therefore, it appears that while the KDOL was effective at flagging potentially fraudulent claimants, it flagged a number of likely legitimate claimants as well.

Evaluating the Impact of Waiving the One-Week Waiting Period

We understand that prior to March 30, 2020, a one-week waiting period was required to give KDOL more time to adjudicate and investigate potential issues with a claim. However, during most of the scope period, this requirement was waived. To assess the potential impact of this decision, we isolated claimants that met certain criteria consistent with a claimant that might not have been paid had this waiting period been in effect. Specifically, we assumed that if a claimant met all of the following criteria, then it is possible that KDOL might have identified the claimant as potentially fraudulent and stopped issuing payments during the one-week waiting period.

1) Claimant had received only a single payment.
2) The benefit period begin date on the claim was six days prior to the first claim week date associated with the single payment, indicating waiver of the one-week waiting period (rather than 13 days which was normal before the waiver).
3) The single payment occurred within seven days of the claim week date. This seemed like a reasonable assumption since most payments happened within seven days, and this is the same number of days as the waiting period. For payments that were delayed longer than seven days, presumably payment would have been stopped regardless of whether the one-week waiting period was in effect.
4) KDOL had flagged the claimant as potentially fraudulent, suggesting that the reason there was only a single payment to the claimant was that KDOL may have stopped payment as opposed to the claimant having stopped filing additional claims.
5) We had identified the claimant as potentially fraudulent in this report.

A total of approximately $15 million was paid to claimants meeting all of these criteria, and as such, might have been avoided but for the waiver of the one-week waiting period.

Employer Analytics

We examined the claim counts by employer in 2015 through 2019 compared with January 2020 through March 2022. First, we identified employers with no claim activity noted prior to 2020 but at least one claim between January 2020 and March 2022. Of the 1,536,416 claims we were able to match between the individual claim level data and the summary level employer data, 712,324, or 46%, matched this pattern. The average score for these claimants was 25, which is the same as the overall population average of 25 and well below the self-reported fraud average of 40. Next, we identified employers with at least twice as many claims during January 2020 through March 2022 as compared with 2015 through 2019. There were 711,463 claims, or 46%, associated with these employers. We searched for correlations between the percentage change between these two periods and risk scores but did not note any strong correlations. The average score for these claimants was 22. We also noted that analyzing specific employer claims prior and during the pandemic was difficult as not all types of employers were impacted the same during the pandemic.

Improper Payments

We obtained detail of overpayments by claimant from KDOL. We have summarized this detail in Figure 8 below, by category of overpayment. The totals below were labeled as "Total Due" in the spreadsheet provided to us. The left column provides totals which include claimants which we have identified in this report as potentially fraudulent. The right column provides totals which exclude those claimants.

Figure 8

OVERPAYMENT REASON	Total Including Flagged Claimants	Total Excluding Flagged Claimants
Attributing earnings to wrong week	$ 6,966.64	$ 5,828.00
Bank pay award	$ 87,344.84	$ 87,344.84
Clerical or CSR/Adjudicator error	$ 1,023,133.64	$ 934,724.14
Concurrent filing against two states	$ 296,901.47	$ 287,805.46
EDP program error	$ 947.20	$ 947.20
Error in computing weekly or maximum amount	$ 375.00	$ 375.00
Failure to act on disqualifying information	$ 224,689.52	$ 202,051.52
Illegal alien	$ 910,134.79	$ 797,837.07
Inadequate search for work	$ 555,855.29	$ 539,987.29
Incorrect reason for separation	$ 23,355,720.03	$ 19,200,337.31
Incorrect reporting of base period wages	$ 1,150,196.74	$ 963,642.12
Incorrect reporting of weeks of work	$ 8,934.68	$ 7,630.68
Keypunch error	$ 60,887.00	$ 60,821.00
Not elsewhere classified-attributable to agency	$ 5,186,734.12	$ 4,654,946.00
Not elsewhere classified-attributable to the claim	$ 5,457,605.71	$ 3,639,391.18
Not elsewhere classified-attributable to the emplo	$ 75,872.12	$ 74,122.12
Payment after failure to report	$ 8,258,258.38	$ 6,911,550.66
Reasonable assurance	$ 305,514.64	$ 254,826.64
Refused to accept suitable work	$ 1,340,886.91	$ 1,246,157.40
Reporting of business owner wages	$ 1,440.00	$ 1,440.00
Reversal (JAVA)	$ 2,049,892.86	$ 1,943,105.86
Reversal (other than JAVA)	$ 9,797,735.94	$ 9,038,723.84
Unable or unavailable for work	$ 7,166,966.64	$ 5,943,150.75
Underreporting of wages	$ 318,837.56	$ 304,976.39
Unreported Worker's Compensation	$ 101,329.30	$ 100,353.30
Unreported irregular separation	$ 2,413,010.42	$ 2,005,585.58
Unreported pension	$ 462,936.52	$ 412,129.84
Unreported vacation/holiday pay/severance	$ 2,837,994.54	$ 2,437,573.72
Unreported wages	$ 3,630,478.66	$ 3,216,741.96
Multiple Reasons	$ 638,804.38	$ 618,059.14
	$ 77,726,385.54	**$ 65,892,166.01**

Passwords and Security Phrases

We asked for passwords and security phrases associated with claimants to use in our analysis but were told by KDOL that they are no longer retained by KDOL at the advice of a security audit they had undergone.

Comparison between 2020 and 2021

Total payments in 2020 and 2021 were $2,507,087,871 and $839,771,851, respectively. These totals are broken down by program in Figure 9 below.

Figure 9

Program	2020	2021
UI REGULAR	$ 979,770,296	$ 319,533,891
EB	$ 11,898,953	$ 1,658,337
MEUC	$ -	$ 85,380
PUA	$ 177,615,809	$ 36,730,814
FPUC	$ 1,226,085,098	$ 318,339,932
PEUC	$ 110,859,636	$ 161,838,230
TRA	$ 858,079	$ 1,585,267
	$ 2,507,087,871	**$ 839,771,851**

The number of claims in 2020 and 2021 were 1,030,801 and 472,442 respectively. There were 669,759 claimants with one or more claims in 2020 but none in 2021. There were 335,976 claimants with one or more claims in 2021 but none in 2020. There were 65,738 claimants with claims in both 2020 and 2021.

There were 222,375 claimants who received at least one payment in 2020 but none in 2021. There were 120,754 claimants who received at least one payment in both 2020 and 2021. There were 70,514 claimants who received at least one payment in 2021 but none in 2020.

KDOL Progress on implementation of program integrity elements

FORVIS was asked to assess KDOL's progress on implementing the program integrity elements and guidance issued by the United States Department of Labor and the National Association of State Workforce Agencies. The following integrity elements and guidance are included along with a brief assessment of KDOL's progress in these areas. Our assessment of these areas is based on discussions with KDOL personnel.

A. Social security administration cross-matching for the purpose of validating social security numbers supplied by a claimant.

KDOL performed procedures related to validating social security numbers (SSN) both prior to and during the pandemic. During the height of the pandemic, KDOL staff continued to perform procedures around SSN verification, testing that ordinarily would have been done during the one-week waiting period. We understand from our discussions with KDOL, that the ability to keep up with all fraud testing elements was challenging due to the unprecedented volume of claim filings.

KDOL is currently in the process of implementing Pondera Solutions (Pondera), a fraud detection software that utilizes advanced data analytics to identify potential fraud. Pondera will utilize data, including SSN data to better automate the Department's fraud detection capabilities going forward.

B. Checking of new hire records against the national directorate of new hires to verify eligibility.

We understand from our discussions with KDOL that this procedure has been in place throughout the pandemic. Similar to SSN cross-matching procedures, KDOL's ability to sustain its fraud detection capabilities during the height of the pandemic was impacted by the significant growth in claim filings.

C. Verification of immigration status or citizenship and confirmation of benefit applicant information through the systematic alien verification for entitlement program.

We understand from our discussions with KDOL, claimants are required to acknowledge their immigration status on their unemployment insurance claim application. Depending on the claimants' responses in their application KDOL follows up. KDOL also relies on the fact that employers are required to check immigration status. KDOL does not currently utilize any external data to verify immigration status.

D. Comparison of applicant information to local, state, and federal prison databases through incarceration cross-matches.

Prior to and since the beginning of the pandemic, KDOL has been utilizing data from the Kansas Department of Corrections to identify potentially fraudulent claims. One limitation on the data was that KDOL had been provided with prison release information but had not been incorporating that information into its process or saving that data beyond a three-week retention period. This could have led to falsely flagging an individual if they had been released from prison and became eligible for unemployment insurance. We made KDOL aware of this limitation, and we have been told they have begun retaining prison release information on a go forward basis. KDOL has not had access to federal prison records, but we understand that with the implementation of Pondera, KDOL will now have access to federal prison databases to supplement its searches within the state of Kansas.

E. Detection of duplicate claims by applicants filed in other states or other unemployment insurance programs through utilization of the interstate connection network, interstate benefits cross-match, the state identification inquiry state claims and overpayment file and the interstate benefits 8606 application for overpayment recoveries for Kansas claims filed from a state other than Kansas.

- We understand from our discussions with KDOL that currently and historically, KDOL has not been able to develop an automated process for identifying possible claimants filing inappropriately in multiple states. KDOL utilizes ICON and Integrity Data Hub (IDH) to search for possible problematic claims. ICON utilizes data from the State Wage Record

Exchange System to identify claimants with wages paid in other states. When a claimant files on-line there is no automated check against filings in other states. This is a system limitation KDOL will rectify during modernization. The claimant application does require claimants to note if they have filed in other states. A yes response to that question results in additional research; however, the approach to flagging claimants that have filed in multiple states is manual.

F. Identification of internet protocol addresses linked to multiple claims or to claims filed outside of the United States.

KDOL has not fully developed its approach to incorporating IP address testing into its fraud analytics program. KDOL currently has procedures to block payment on claims with foreign IP addresses.

G. Use of data mining and data analytics to detect and prevent fraud when a claim is filed, and on an ongoing basis throughout the lifecycle of a claim, by using current and future functionalities to include suspicious actor repository, suspicious email domains, foreign internet protocol addresses, multi-state cross-match, identity verification, fraud alert systems and other assets provided by the unemployment insurance integrity center.

As discussed above, KDOL is in the process of implementing Pondera which will allow KDOL to improve its ability to perform proactive data mining and data analytics to assist with detecting and preventing the payment of fraudulent claims. Pondera will streamline KDOL's process to monitor claims and utilize third party data sources to enhance its ability to identify fraudulent claims.

Assessment of the KDOL Phone System

We obtained policies and procedures for phone contacts, read the Legislative Post Audit reports, and inquired of management on processes in place during the Period. There were significant delays in phone response times due to the substantial volumes of calls placed to KDOL because of the new legislation and benefits. KDOL onboarded personnel from other departments and agencies to assist with responding to the significant increase in the volume of calls during the early days of the pandemic. According to our inquiry, the hold times could be well over an hour during the peak call periods. Due to the wait times experienced to contact a customer service person, it is highly unlikely that fraudulent callers would wait on-hold and answer the CSR questions and successfully file a fraudulent claim. We ascertained that KDOL made enhancements subsequently to increase the number of verification questions to increase the reliability of a valid claim. Our data analysis above indicates that, although there were a significant number of claims initiated by phone, the potentially fraudulent claims were more likely to have been filed online. As noted above, 98.5% of the potentially fraudulent claims identified were filed via the internet, and approximately 1.5% were filed by phone.

Leadership and Personnel Changes at KDOL

KDOL has experienced significant leadership changes throughout the Period. KDOL provided the following timeline with respect to the leadership positions at the Department.

Secretary of Labor

- Secretary of Labor Delia Garcia's last official day in office was Friday, June 19, 2020.
- Ryan Wright, Deputy Chief of Staff, Governor's Office was interim Secretary of Labor from June 22, 2020, through December 21, 2020.
- Brett Flaschbarth, then Deputy Secretary of KDOL, was named Interim Secretary of Labor from December 22, 2020 through January 27, 2021. Mr. Flaschbarth resigned his position as Deputy Secretary effective June 19, 2021.
- Amber K. Shultz was appointed Secretary of Labor beginning January 27, 2021 and remains Secretary to the present day.

Deputy Secretary of Labor

- Peter Brady was Deputy Secretary of Labor from August 2, 2020 through August 12, 2022. Prior to his role as Deputy Secretary, Peter was Director of Industrial Safety and Health.
- Keith M. Tatum was hired as Deputy Secretary of Labor beginning May 2, 2022 and remains in that role.

Chief of Staff

- Sandy Johnson was hired as Chief of Staff beginning April 18, 2021.

Chief Information Officer

- John Cahill, Chief Information Officer departed KDOL May 3, 2020.
- Bill Periman, Chief Information Officer was in this role from July 1, 2020 to November 13, 2020.
- Kelly Johnson was Interim Chief Information Officer from December 31, 2020 through February 20, 2021, and Chief Information Officer from February 21, 2021 through June 25, 2022.
- Doug Eamigh has been interim Chief Information Office from June 26, 2022 to the present.

Recommendations

Automated Potential Fraud Flagging Process

KDOL utilized a mixture of automated and manual procedures to identify potentially fraudulent claims during the scope period. We recommend KDOL implement automated processes to identify potentially fraudulent claims. We understand that KDOL is currently in the process of implementing Pondera, a fraud detection software that utilizes advanced data analytics to identify potential fraud.

Track Specific Reasons for Potential Fraud Flag

KDOL used a generic flag for claims suspected to be potentially fraudulent during the scope period. This limited our ability to analyze the effectiveness of their potential fraud flagging process and did not allow us to analyze the specific types of fraud flags that could have been used. We recommend identifying the specific reasons why claims were flagged as potentially fraudulent. This will allow KDOL to assess the effectiveness of individual potential fraud flag and identify patterns and possible trends, including potential emerging fraud schemes.

Analyze Effectiveness of Specific Potential Fraud Flags

In addition to tracking the specific reasons for potential fraud, we recommend KDOL periodically analyze these specific potential fraud flags to assess their effectiveness, at some meaningful interval, but not less frequently than annually. This assessment should consider the predictive capability of the specific potential fraud flags relative to claims determined to be fraudulent. KDOL should also develop new fraud flags periodically to address emerging fraud schemes.

Continue Use of Kansas Unemployment Insurance Fraud Reporting Tool

We recommend continuing the use of the online Kansas unemployment insurance fraud reporting tool at https://reportfraud.ks.gov/. Even the best analytics cannot identify all potentially fraudulent claims and augmenting those procedures with the ability to self-report fraud is helpful to not only identify potential fraudulent claims, but also have data which can be used to evaluate the effectiveness of existing analytical procedures and identify potential new analytical procedures.

Create a Process to Identify New Analytical Procedures

In an ever-changing world where fraudsters are constantly inventing new ways to circumvent controls, being vigilant and identifying new analytical procedures to identify new schemes is advised. We recommend studying the self-reported fraud claims and other claims which were not flagged by analytics to gain an understanding of the nature of the claim to determine whether a new analytic should be developed to catch similar potentially fraudulent claims. In addition, we recommend holding recurring meetings with other state unemployment agencies to share fraud prevention techniques.

Retain and Utilize Kansas Department of Corrections Prison Release Date

KDOL did not retain the prison release date for state incarceration records during the scope period to determine whether a claimant had simply been incarcerated at some point prior to the claim filed date, or whether the claimant was incarcerated as of the date of the claim filed date. We recommended, and have been told, that KDOL has since began retaining the prison release date.

Documentation of Procedures

Once new procedures have been implemented, we recommend these procedures be documented which will help to keep KDOL team members synchronized, improve consistency during periods of turnover, enhance training and allow third parties, such as auditors, to have greater clarity and understanding of the procedures KDOL has implemented. This documentation should be updated periodically, and information about which procedures were implemented on which dates, modified on which dates, and discontinued on which dates should be retained.

Training

Leveraging the documented procedures described above, training of new employees should be conducted to ensure consistency of application of procedures. Training should be periodic and should incorporate lessons learned from the pandemic and updated to incorporate emerging fraud schemes.

Attachment A – Scope of Work From the Request for Proposals

Scope of Work – Base Bid

FORVIS shall understand the effects on the Kansas Department of Labor and the unemployment insurance system of fraudulent claims and improper payments during the period of March 15, 2020 through March 31, 2022, and the response by the Kansas Department of Labor to such fraudulent claims and improper payments during that period.

The scope of services shall include:

1) An assessment of systems with access to the payment and processing of claims, forensic endpoint images related to the claims and the external perimeter housing the claims systems, as well as an assessment of the Kansas Department of Labor's response to claims. (Due May 1, 2022)

2) The amounts and nature of improper payments and fraudulent claims, fraud processes and methods and the possibility of recovery of any improper payments. The term “improper payment” means any payment that should not have been made or that was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements and includes any payment to an ineligible recipient. Distinguish improper payment from fraudulent claims. Compile, assess and evaluate a statistically significant, projectable, and time-line controlled sample of State Unemployment Insurance Trust Fund funded programs of fraudulent claims and improper payments. Statistically significant and projectable sampling shall be made for each quarter of calendar years 2020 and 2021, and the first quarter of calendar year 2022. (Due September 1, 2022)

    a. Address whether such improper payments were made pursuant to pandemic-related federal unemployment compensation programs or the state’s traditional unemployment compensation program.

    b. Address whether such claims were made prior to or after the implementation of multi-factor authentication methods by the Kansas Department of Labor.

    c. Assessment of the frequency of claimant profile password changes, PIN resets and whether common PINs are allowed (1111, 1234, etc.).

    d. Assessment of the claimant payment method used for such claims and payments.

    e. Assessment of the amount of such payments that may have been avoided if the unemployment waiting week had not been waived as of March 31, 2020.

    f. Assessment of the factors used by the Kansas Department of Labor to flag a claim for fraud and the effectiveness and accuracy of each such factor.

3) An assessment that provides likelihood of a data breach within the Kansas Department of Labor, being a contributing factor to any fraudulent payments, improper network architecture allowing a potential breach to have occurred and a timeline of relevant events. Examine additional possible avenues for which fraudulent activities could have occurred within the Unemployment Insurance Program to include, but not limited to, the human factor related to fraud and data breaches. This assessment should include a review of whether the Kansas Department of Labor had controls to ensure staff were properly background checked and trained in IT security to ensure the security of sensitive unemployment insurance information and whether those controls followed during the COVID-19 pandemic. (Due September 1, 2022)

4) Information on the progress regarding the secretary's implementation of all program integrity elements and guidance issued by the United States Department of Labor and the National Association of State Workforce Agencies (due September 1, 2022). Those elements include:

    a. Social security administration cross-matching for the purpose of validating social security numbers supplied by a claimant.

b. Checking of new hire records against the national directorate of new hires to verify eligibility.

c. Verification of immigration status or citizenship and confirmation of benefit applicant information through the systematic alien verification for entitlement program.

d. Comparison of applicant information to local, state, and federal prison databases through incarceration cross-matches.

e. Detection of duplicate claims by applicants filed in other states or other unemployment insurance programs through utilization of the interstate connection network, interstate benefits cross-match, the state identification inquiry state claims and overpayment file and the interstate benefits 8606 application for overpayment recoveries for Kansas claims filed from a state other than Kansas.

f. Identification of internet protocol addresses linked to multiple claims or to claims filed outside of the United States.

g. Use of data mining and data analytics to detect and prevent fraud when a claim is filed, and on an ongoing basis throughout the lifecycle of a claim, by using current and future functionalities to include suspicious actor repository, suspicious email domains, foreign internet protocol addresses, multi-state cross-match, identity verification, fraud alert systems, and other assets provided by the unemployment insurance integrity center.

Scope of Work – Additional Items

1) Assessment of the phone system used by the Kansas Department of Labor to respond to claimant and assist claimants in filing claims.

2) Assessment of the number of unique individual claimants receiving benefits by unemployment compensation program in 2020 and 2021 and the total number of claims, and amount of benefits, paid to each individual.

3) Assessment of the employer claim counts and charges for the five years preceding 2020 and claims in 2020 and 2021, with an examination of employers showing large increases in 2020 and 2021 to determine how many fraudulent claims were not flagged for fraud. Assess fictitious employer scheme fraud claims for the five years preceding 2020 and including 2020 and 2021. Fictitious employer schemes may include, but not limited to, creation of fictitious companies, use of post office box addresses, no actual employees, business operations or normal business expenses.

4) Make recommendations for future Unemployment Insurance Systems and Practices.

5) Assess and note timeframes of leadership and personnel changes at the Kansas Department of Labor. Assess administration changes, and whether policies, security, protocols, and guidelines changed. Assess crucial milestones and the impact they had on fraudulent and improper payment claims. Assessment and notation of timeframes and crucial milestones shall be for the period between March 15, 2020, and March 31, 2022.