# Department of Labor

## Controls and Management of the Unemployment Insurance System

Report 2021-S-3 | November 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller
Division of State Government Accountability

# Audit Highlights

## Objective

To determine whether the Department of Labor (Department) has taken appropriate steps to oversee and manage the Unemployment Insurance system and to comply with selected portions of the New York State Information Security Policy and Standards. The audit covered the period from January 2020 to March 2022.

## About the Program

The Department's mission is to protect workers, assist the unemployed, and connect jobless workers to jobs. One of its key tasks in assisting the unemployed is administering the State's Unemployment Insurance (UI) program. The UI program is a joint federal–State initiative that provides benefits to eligible workers who become unemployed through no fault of their own (as determined under State law) and meet other eligibility requirements of State law. In March 2020, Executive Order 202.8 – New York State on PAUSE – directed the temporary closure of all non-essential businesses statewide to mitigate the spread of COVID-19. In addition, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), also enacted in March 2020, created temporary programs that allowed for enhanced UI benefits for those affected by COVID-19. The COVID-19 pandemic and the addition of temporary benefit programs, like Pandemic Unemployment Assistance (PUA) which had less stringent requirements than traditional UI, contributed to a dramatic increase in UI claims. Collectively, these factors not only increased the demand for as well as the amount of UI benefits but also increased the risk of improper payments and fraud, largely the result of identity theft.

Further, even without considering claims from the temporary federal programs, according to information derived from the federal Benefit Accuracy Measurement (BAM) program and reported on the U.S. Department of Labor (USDOL) website, for the period April 1, 2021 to March 31, 2022, the estimated fraud rate in New York's UI program increased to 17.59% – up from 4.51% just 2 years earlier.[1] Prior to and during the pandemic, the Department performed matches of applicant information against databases from agencies such as the Social Security Administration and the Department of Motor Vehicles to assist in verifying applicants' identity and eligibility and identify potentially fraudulent claims. Department officials also added new protocols to assist with identifying fraudulent claims, particularly those attributed to identity theft. In February 2021, the Department began using ID.me, Inc. (ID.me) to provide identity verification services.

In addition to managing UI benefits and record claim volumes during the pandemic, Department officials were still responsible for maintaining the UI system in accordance with appropriate standards, including those issued by the Office of Information Technology Services (ITS). As the owner of UI system data, the Department is responsible for classifying the data in its systems, determining the commensurate controls, and ensuring the controls are in place as needed. ITS maintains the Department's systems and is responsible for implementing those controls.

[1] BAM is a statistical survey that, among other things, estimates state UI improper payments and is used by the USDOL. It is required by the Improper Payments Information Act and the Elimination and Recovery Act. The BAM survey sample (random audits) includes paid claims in three major UI programs: State UI, Unemployment Compensation for Federal Employees, and Unemployment Compensation for Ex-Service Members. The USDOL has not yet estimated amounts of improper payments and fraud for the pandemic UI programs (e.g., PUA and Mixed Earner Unemployment Compensation).

From April 1, 2020 through March 31, 2021, the Office of the State Comptroller authorized more than 218.2 million UI payments totaling over $76.3 billion – an increase of nearly 3,140% over the amount of payments authorized in the prior fiscal year.

## Key Findings

- Overall, we found deficiencies with the Department's oversight and management of its UI system that ultimately compromised its ability to effectively mitigate risks related to the processing of claims – fraudulent claims in particular – and system and data security.
- During the pandemic, faced with the high demand for UI benefits and the need to process claims quickly, the Department resorted to stop-gap measures to compensate for system limitations, which ultimately proved to be costly to the State. We found its workarounds resulted in misclassification of claims as State instead of federal liabilities, overpayment of claims, and supplemental spending to maintain the outdated UI system infrastructure while the new system was in development.
- Department officials were unable to provide us with granular data or analyses to support their management of and response to fraudulent claims on the UI system, including:
  - Support for $36 billion in fraudulent claims reported by the Department as prevented;
  - The number of claims that were actually paid to fraudulent claimants before being detected;
  - The length of time from when claims were filed to when they were identified as fraudulent (to determine the number of weeks that payments were made); and
  - How the claims were originally identified as fraudulent (e.g., whether through departmental procedures or based on complaints from individuals whose identities were used by impostors to file false claims).
- Department officials could not provide supporting information for or otherwise explain why the estimated fraud rate derived from the federal BAM program for the Department's traditional UI increased more than threefold during State fiscal year 2020-21, nor could they provide information on certain performance measures related to the implementation of the ID.me identity verification service.
- The Department did not take some fundamental, critical steps established in the Security Policy and the Classification, Encryption, Authentication, and Logging Standards to secure its UI system and data. As a result, the Department has minimal assurance that its substantial information assets are protected against loss or theft.
- The Department's slow response to certain requests – in some cases up to 6 months after the fact – delayed our findings and recommendations and, in turn, the Department's ability to promptly address serious problems.

## Key Recommendations

- Continue the development of the replacement UI system and ensure its timely implementation.
- Take steps, including collecting and analyzing data related to the identity verification process, to ensure the correct balance between fraudulent identity detection and a streamlined process for those in need of UI benefits.

- Follow up on the questionable claims identified by our audit to ensure adjustments have been made so they are paid from the proper funding source and overpayments are recovered, as warranted.
- Ensure the current and new UI system and data comply with provisions of the Security Policy, the Classification, Authentication, Encryption, and Logging Standards, as well as the Change Management Process and Policy.
- Improve the timeliness of cooperation with State oversight inquiries to ensure transparent and accountable agency operations.

**Office of the New York State Comptroller**
**Division of State Government Accountability**

November 15, 2022

Roberta Reardon
Commissioner
Department of Labor
W. A. Harriman State Campus, Building 12
Albany, NY 12240

Dear Commissioner Reardon:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Controls and Management of the Unemployment Insurance System*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

*Division of State Government Accountability*

# Contents

# Glossary of Terms

| Term | Description | Identifier |
|---|---|---|
| Department | Department of Labor | *Auditee* |
| | | |
| Authentication Standard | Authentication Tokens Standard NYS-S14-006 | *IT Standard* |
| BAM | USDOL Benefit Accuracy Management | *Key Term* |
| Budget Hearings | 2022-23 Joint Legislative Budget Hearings on Workforce Development | *Key Term* |
| CARES Act | Federal Coronavirus Aid, Relief, and Economic Security Act | *Key Term* |
| Classification Standard | Information Classification Standard NYS-S14-002 | *IT Standard* |
| 2021 Comptroller's Report | *Unemployment Insurance Trust Fund: Challenges Ahead* | *Key Term* |
| Encryption Standard | Encryption Standard NYS-S14-007 | *IT Standard* |
| IAS | Interest Assessment Surcharge | *Key Term* |
| ID.me | ID.me, Inc. | *Key Term* |
| Information Security Controls Standard | Information Security Controls Standard NYS-S14-003 | *IT Standard* |
| ITS | Office of Information Technology Services | *State Agency* |
| LEP | Limited English Proficient | *Key Term* |
| Logging Standard | Security Logging Standard NYS-S14-005 | *IT Standard* |
| May 2021 USDOL Report | *COVID-19: States Struggled to Implement CARES Act Unemployment Insurance Programs,* issued May 28, 2021 | *Key Term* |
| NIST | National Institute of Standards and Technology | *Key Term* |
| NIST 800-53 | NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations | *IT Standard* |
| OSI | The Department's Office of Special Investigations | *Key Term* |
| PEUC | Pandemic Emergency Unemployment Compensation | *Key Term* |
| PIIA | Payment Integrity Information Act of 2019 | *Key Term* |
| Plan | Language Access Plan | *Key Term* |
| PUA | Pandemic Unemployment Assistance | *Key Term* |
| RBAC | Role-based access control | *Key Term* |
| Security Policy | Information Security Policy NYS-P03-002 | *IT Standard* |
| Standards | Standards for Internal Control in New York State Government | *Standard* |
| UI | Unemployment Insurance | *Key Term* |
| USDOL | U.S. Department of Labor | *Federal Agency* |

# Background

The Department of Labor's (Department) mission is to protect workers, assist the unemployed, and connect jobless workers to jobs. One of its key tasks in assisting the unemployed is administering the State's Unemployment Insurance (UI) program. The UI program is a joint federal–State initiative that provides benefits to eligible workers who become unemployed through no fault of their own (as determined under State law) and meet other eligibility requirements of State law. UI benefits are paid with federal and State taxes collected from employers, and UI eligibility, benefit amounts, and the length of time benefits are available are determined by State law. The State's UI system is made up of 94 subsystems that serve different functions, such as managing applications, processing benefits, and tracking employer contributions. (For purposes of this report, we refer to these subsystems collectively as the "UI system.")

Over time, the federal government has made changes to UI and workforce programs. In addition to implementing these changes, the State has faced the pressing problem of maintaining, modifying, and extending outdated and expensive mainframe-based UI benefits and contributions systems that were written in the 1970s and 1980s, and remains constrained by the technology of that era. As noted by the Pandemic Response Accountability Committee in its December 2021 report, "Key Insights: State Pandemic Unemployment Insurance Programs," the National Association of State Workforce Agencies found that over half of states were relying on outdated unemployment computer systems as of February 2021.

In March 2020, Executive Order 202.8 – New York State on PAUSE – directed the temporary closure of all non-essential businesses statewide to mitigate the spread of COVID-19. Other executive orders issued in response to the pandemic directly affected the UI program, making it easier for New Yorkers impacted by the forced business closures to receive benefits. For example, one such order temporarily waived the 1-week waiting period for unemployment benefit payments, thereby expediting funds to those in need but also reducing the time available for the Department to verify claimants' eligibility for benefits and claim information. In addition, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), also enacted in March 2020, created temporary programs that allowed for enhanced UI benefits for those affected by COVID-19:

- Pandemic Unemployment Assistance (PUA), which provided up to 79 weeks of UI benefits for individuals who were unable to work due to COVID-19 but who did not qualify for traditional UI, such as the self-employed;
- Pandemic Emergency Unemployment Compensation (PEUC), which provided individuals with 53 additional weeks of UI benefits after their State's benefits have run out;
- Extended Benefits, which provided up to 20 additional weeks of benefits after all 26 weeks of traditional UI benefits and all 53 weeks of PEUC benefits have been exhausted; and

- Federal Pandemic Unemployment Compensation, a $600 weekly unemployment compensation boost (later reduced to $300) for certain eligible individuals.

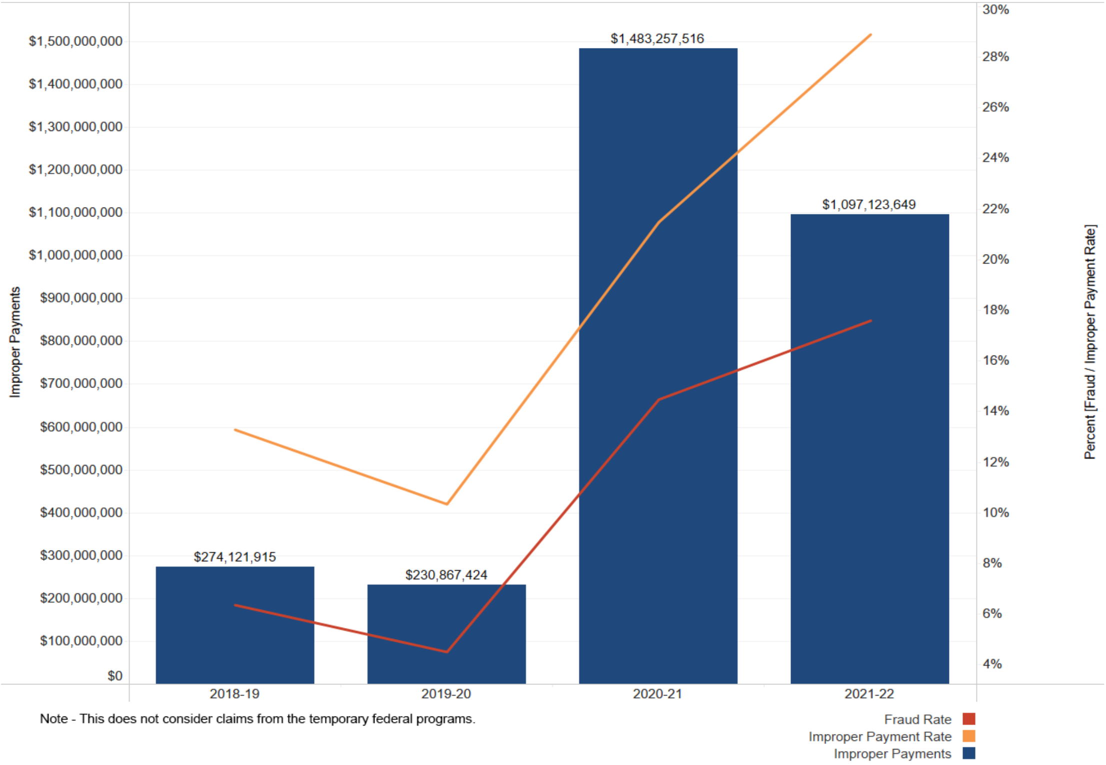
The pandemic and the addition of these temporary benefit programs created under the CARES Act contributed to a dramatic increase in UI claims. From April 1, 2020 through March 31, 2021, OSC authorized more than 218.2 million UI payments totaling over $76.3 billion – an increase of nearly 3,140% over the amount of payments authorized in the prior fiscal year.

The record claim volume stemmed not only from the expanded eligibility and extended benefits from the CARES Act program but also the less stringent requirements to qualify for certain UI benefits. Collectively, these factors not only increased the demand for UI benefits but also increased the risk of improper payments and fraud. For example, the CARES Act allowed claimants under these temporary programs to self-certify their eligibility and wages and required states to make immediate eligibility determinations. As the U.S. Department of Labor (USDOL) Inspector General commented in its semi-annual report to Congress covering the period April 1, 2020 through September 30, 2020, "The sole reliance on claimant self-certifications without evidence of eligibility and wages renders the PUA program vulnerable to improper payments and fraud." The USDOL has not yet estimated amounts of improper payments and fraud for the pandemic UI programs (e.g., PUA and Mixed Earner Unemployment Compensation). However, even without considering claims from the temporary federal programs, according to information derived from the federal Benefit Accuracy Measurement (BAM) program and reported on the USDOL website, for the period April 1, 2021 to March 31, 2022, the estimated fraud rate in New York's UI program increased to 17.59% – up from 4.51% just 2 years earlier (see Figure 1).

The pandemic created a dual mandate for the Department. Under the CARES Act, the Department was mandated to make quick eligibility determinations using information self-certified as accurate by UI applicants, while still striving to meet the UI payment integrity requirements. The Payment Integrity Information Act (PIIA) of 2019 requires UI programs to report an annual improper payment rate below 10%, and the federal UI program established a performance measure for states to meet the 10% requirement. According to information on the USDOL website, even prior to the pandemic, New York's UI program exceeded the 10% PIIA threshold. Prior to the pandemic for State fiscal year (SFY) 2018-19, the State's estimated improper payment rate for the UI program was 13.28% and in 2019-20 it was 10.34%. For SFY 2020-21, at the height of the pandemic, the improper payment rate increased to 21.48%[2] and continued to increase to 28.89% in 2021-22, as shown in Figure 1.

[2] Reporting was suspended from the end of March 2020 through the end of June 2020 according to data warning notes on the Department's website. Consequently, figures for SFY 2020-21 represent three quarters of data.

**Figure 1 – Estimated Improper UI Payment and Fraud Rates, 2018–2022**



Note - This does not consider claims from the temporary federal programs.

The increase in improper payments and fraud was largely the result of identity theft. Prior to and during the pandemic, the Department performed matches of applicant information against databases from agencies such as the Social Security Administration and the Department of Motor Vehicles to assist in verifying applicants' identity and eligibility and identify potentially fraudulent claims. In fact, the Department performed the three matches required by the USDOL and seven of its eight recommended matches for UI applicants. However, individuals as well as criminal networks recognized opportunities to take advantage of the new temporary programs' lax requirements by submitting fraudulent claims with stolen identities. The risk of stolen identities being used to apply for government benefits was highlighted in a 2019 report from the U.S. Government Accountability Office following the 2017 Equifax data breach.[3] According to Department officials, a key challenge of the sudden increase in fraud using stolen identities was that since the identities were real, albeit used fraudulently, they would still likely pass the data matches that had been in place. Throughout the pandemic, according to Department officials, they developed queries to analyze application information that fit ever-changing fraud and abuse patterns. Department officials also provided a list of protocols added to assist with identifying fraudulent claims, particularly those attributed to identity theft. In August 2020 – more than 4 months after the CARES Act temporary benefit programs were authorized – officials started considering additional solutions to assist them

[3] U.S. Government Accountability Office: Data Protection - Federal Agencies Need to Strengthen Online Identity Verification Processes

in better detecting and eliminating fraudulent applications based on identity theft. The Department contracted with ID.me, Inc. (ID.me) to provide identity verification services. The Department implemented these services in February 2021, nearly a full year after the new temporary benefit programs were put in place. See Exhibit for a timeline of events. In addition to managing UI benefits and record claim volumes during the pandemic, Department officials were still responsible for maintaining the UI system in accordance with appropriate standards, including those issued by the Office of Information Technology Services (ITS). All State entities, including the Department, must follow ITS' security policies and standards related to security and account management and access controls.

ITS' Information Security Policy NYS-P03-002 (Security Policy) – the principal policy that governs all other ITS security policies and associated standards – defines the mandatory minimum information security requirements for all State entities, including the Department, to ensure a secure and stable IT environment. The Security Policy framework is the basis for ensuring that appropriate measures are in place to protect the confidentiality, integrity, and availability of information assets, and that staff and all other affiliates understand their roles and responsibilities; have adequate knowledge of security policies, procedures, and practices; and know how to protect State entity information. The Security Policy encompasses all systems, automated and manual, for which New York State has administrative responsibility, and addresses all information, regardless of form or format, that is created or used to support the business activities of State entities. Additionally, the Security Policy states that advance planning and preparation must be performed to ensure the availability of adequate capacity and resources, and system capacity must be monitored on an ongoing basis.

Other ITS-issued standards, frameworks, and procedures govern specific security-related scenarios. These include the Information Classification Standard NYS-S14-002 (Classification Standard), Encryption Standard NYS-S14-007 (Encryption Standard), Authentication Tokens Standard NYS-S14-006 (Authentication Standard), Security Logging Standard NYS-S14-005 (Logging Standard), Information Security Controls Standard NYS-S14-003 (Information Security Controls Standard), and the ITS Change Management Process and Policy. The ITS policies and standards are also based, in part, on standards issued by the National Institute of Standards and Technology (NIST), including Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations (NIST 800-53).

As the owner of UI system data, the Department is responsible for classifying the data in its systems, determining the commensurate controls, and ensuring the controls are in place as needed. ITS maintains the Department's systems and is responsible for implementing those controls.

# Audit Findings and Recommendations

Overall, we found deficiencies with the Department's oversight and management of its UI system that ultimately compromised its ability to effectively mitigate risks related to the processing of claims – fraudulent claims in particular – and system and data security.

Department officials did not heed warnings as far back as 2010 that the UI system was out of date and, consequently, difficult to maintain and that it lacked the agility necessary to adjust to new laws and the scalability to handle workload surges. During the pandemic, faced with the high demand for UI benefits and the need to process claims quickly, the Department resorted to stop-gap measures to compensate for system limitations, which ultimately proved to be costly to the State. We found its workarounds resulted in misclassification of claims as State instead of federal liabilities, overpayment of claims, and supplemental spending to maintain the outdated UI system infrastructure while the new system was in development. For instance, Department decisions led to overrides of the automated internal controls in place that enforce the 26-week maximum for traditional UI claims, allowed claimants to be paid from incorrect program funds, and increased the risk that a claimant may be overpaid. Additionally, had the Department been using a more modern system that could more easily be supported by Department and ITS staff, additional costs for specialized services could have potentially been avoided.

Further, the system also presented obstacles to monitoring and analyzing fraudulent claims and for informed operational decision making. For instance, in January 2022, the Commissioner of Labor testified during the 2022-23 Joint Legislative Budget Hearings on Workforce Development (Budget Hearings) that the Department had prevented over $36 billion in fraudulent UI payments. However, during the course of the audit, Department officials were unable to provide us with granular data or analyses to support their management of and response to fraudulent claims on the UI system. Among other critical questions that remain unanswered, officials could not account for the number of claims that were actually paid to fraudulent claimants before being detected; the length of time from when claims were filed to when they were identified as fraudulent (to determine the number of weeks that payments were made); and how the claims were originally identified as fraudulent (e.g., whether through departmental procedures or based on complaints from individuals whose identities were used by impostors to file false claims). In addition, Department officials could not provide supporting information to explain why the estimated fraud rate for its traditional UI increased more than threefold during SFY 2020-21, nor could they provide information on certain performance measures related to the implementation of the ID.me identity verification service.

We also note the Department was unable to incorporate how it tracked applicant language information into its outdated UI system. Therefore, Department officials don't have an easy way to analyze this information to ensure it's in a position to best manage its resources and monitor how it serves Limited English Proficient (LEP) users of the UI system.

The Department is also responsible for operating its current UI system according to ITS policies and standards. Overall, we found the Department has not taken some fundamental, critical steps established in the Security Policy and the Classification, Encryption, Authentication, and Logging Standards to secure its UI system and data. As a result, the Department has minimal assurance that its substantial information assets are protected against loss or theft. For example, we determined the Department did not classify data on its UI system, failed to encrypt certain information, did not enforce strong access controls or authentication rules, and did not have a policy in place to ensure systems logs were monitored. Furthermore, some of its changes to the UI system made in response to the COVID-19 pandemic did not meet all the necessary requirements of the ITS Change Management Process and Policy, intended to ensure the mitigation of risks and minimize disruption of critical services. Collectively, this non-compliance increases the risk for unauthorized access to the UI system and information.

Furthermore, we note that Department officials seemed unfamiliar with certain areas of audit, such as basic security controls, and also were not able to readily produce related records and documentation – information that should have been easily retrievable – or failed to provide it altogether. The Department's slow response to our requests – in some cases up to 6 months after the fact – delayed our findings and recommendations and, in turn, the Department's ability to promptly address serious problems.

## Lack of Supporting Data Related to UI Fraud

During the course of the audit, Department officials were unable to provide us with key information or data analyses to support its management of and response to fraudulent claims on its UI system. Nor could they provide supporting information for or otherwise explain why the estimated fraud rate for its traditional UI increased more than threefold during SFY 2020-21. Lastly, Department officials could not provide information on certain performance measures related to its implementation of the ID.me identity verification service.

The Standards for Internal Control in New York State Government (Standards), issued by the Office of the New York State Comptroller, define monitoring as the ongoing evaluation of internal control components to ascertain whether they are present and functioning. Management should focus monitoring efforts on internal control and achievement of the organization's mission. In addition, a communication system consists of methods and records established to identify, capture, and exchange useful information. Further, information is only useful when it is timely, sufficiently detailed, and appropriate to the user. While we recognize the unprecedented claim volume and pressure the Department was under during the COVID-19 pandemic, it was especially important to capture and evaluate relevant data from the UI system to support its operational decisions and publicly reported figures.

## Oversight of Fraud Claim Information

Department officials could not provide certain claim information needed to track and monitor fraudulent claims on an aggregate basis. In January 2022, the Commissioner of Labor testified at the Budget Hearings that the Department had prevented over $36 billion in fraudulent UI payments, including claims related to the temporary federal programs and traditional UI. According to Department officials, they calculated this amount based on the amount the claimant was entitled to, the length of time benefits would be received, and the applicable UI program the person applied for. They also indicated the $36 billion figure is supported by fraudulent claims information maintained by the Department's Office of Special Investigations (OSI) in its database of claims. Information in the OSI database is used to investigate fraudulent claims and is shared with other government agencies charged with investigating and prosecuting fraudulent activity.

For purposes of this audit, we sought to obtain from the Department statistics and supporting documentation related to these fraudulent claims – information that we expected was useful to the Department's UI oversight and thus readily available, such as:

- Of the $36 billion in claims that was calculated as fraudulent, how much was actually paid out to the fraudulent claimants before being detected;
- How were the claims originally identified as fraudulent by the Department (e.g., whether through departmental procedures or analysis or based on complaints from individuals whose identities were used inappropriately to file claims);
- When were the fraudulent claims filed and when were they detected; and
- How many fraudulent claims due to identity theft were processed from the time the temporary benefit programs began to when ID.me was implemented.

However, Department officials stated the information we sought was not available, nor could it be determined from the OSI database. According to officials, this additional claim information would have to be determined from the detailed claim information on its mainframe system. However, they acknowledged the existing mainframe does not allow for easy aggregation and analysis of the claims data in the OSI database. We requested the OSI database from the Department. However, as of August 2022, officials had not provided it.

Not only could we not verify the accuracy of the Department's claims of $36 billion in fraudulent claims prevented, but, as Department officials stated, the Department cannot accurately determine how many fraudulent claims were actually paid and thus need to be recovered.

## Increase in Traditional UI Fraud Rates

As noted earlier in our report, much of the fraud in UI during the pandemic was attributed to the temporary federal programs, especially PUA. However, even without considering the temporary federal programs, according to the USDOL's BAM program information, as reported on its website, for the period April 1, 2020 to March 31, 2021,[4] the estimated fraud rate increased to 14.48%, up from 4.51% for the same period a year earlier. This threefold increase occurred despite the Department having implemented enhanced protocols during the pandemic to assist with identifying fraudulent claims, particularly those attributed to identity theft. Department officials did not provide an explanation other than to suggest the method of testing under the BAM program used a small sample of claims and cited a data warning in the BAM report that discusses the risks of sampling errors. While we note there are always risks associated with sample testing, that same data warning also indicates the results are based on a 95% confidence interval, meaning the actual rate is expected to lie within 95% of the intervals constructed from repeated samples of the same size and selected in the same manner as the BAM sample. Therefore, we still question the reasons for the rate of increased fraudulent claims in the traditional UI program given the additional protocols enacted by the Department.

During the pandemic, New York borrowed $9 billion from the federal UI trust fund to pay UI claims. At the Budget Hearings, the Commissioner of Labor was questioned as to how much of the approximately $9 billion owed to the federal UI trust fund was for fraudulent claims. While claiming the fraud figure was not nearly the $9 billion balance outstanding, the Commissioner could not provide an estimate. Borrowing from the federal UI trust fund has serious consequences for the businesses operating in New York State. In July 2022, the Department assessed the first annual Interest Assessment Surcharge (IAS) on the outstanding loan incurred during the pandemic and owed to the federal UI Trust Fund. The 2022 assessment rate is 0.23%, or about $27.60 per employee. Minimizing the borrowing by ensuring the borrowed funds aren’t going to pay fraudulent claims would have a direct impact on New York businesses. Unless the federal government chooses to abate all or part of the interest incurred or the principal balance amount is repaid with no more interest accrued, businesses will be required to make annual IAS payments until all interest has been fully paid off.

## Identity Verification Information

To help combat fraudulent claims filed under stolen identities, the Department selected ID.me, Inc. (ID.me), a vendor, to provide identity verification services, and began using the service in February 2021 – nearly a full year after the new temporary benefit programs were put in place. The contract was amended in June 2021 for a total value of $4.7 million. We reviewed documentation related to the Department’s deployment and integration of the ID.me solution into the UI system, and found it was properly approved and tested for use according to the ITS Change Management

[4] BAM is a statistical survey that, among other things, estimates state UI improper payments and is used by the USDOL. It is required by the Improper Payments Information Act and the Elimination and Recovery Act. The BAM survey sample (random audits) includes paid claims in three major UI programs: State UI, Unemployment Compensation for Federal Employees, and Unemployment Compensation for Ex-Service Members. The USDOL has not yet estimated amounts of improper payments and fraud for the pandemic UI programs (e.g., PUA and Mixed Earner Unemployment Compensation).

Process and Policy. However, the Department could have better captured information on the details of its implementation to ensure it not only prevented fraudulent claims but also balanced the ease of access for legitimate applicants.

The implementation of a more thorough identity verification solution like ID.me raises concerns for those legitimate applicants who may not have been able to complete the online identity verification process through ID.me. Under the process, ID.me reports back to the Department those applicants whose identity is verified online. Those who can't verify may take additional steps to prove their identity. Department officials acknowledged the risk of delayed benefits for legitimate applicants who must take additional steps to verify their identity. Further, ID.me itself acknowledged that certain groups may encounter difficulties using its services. In a 2018 white paper, ID.me acknowledged that young, old, less affluent, and recently migrated individuals are particularly disadvantaged when it comes to proving their identity online.

The Standards define monitoring as the ongoing evaluation of internal control components to ascertain whether they are present and functioning. Management should focus monitoring efforts on internal control and achievement of the organization's mission. Monitoring the implementation of a control like ID.me is especially important to ensure that it achieves its fraud prevention outcomes while also protecting the ability of legitimate applicants to apply for the benefits to which they are entitled and to do so as easily as possible. This would include monitoring for factors such as the number of legitimate applicants who could not complete the identity verification process online and those who required additional assistance to verify their identity. To effectively monitor this implementation, the Department must have sufficient detailed information.

During our audit, the Department did not have or could not provide supporting documentation regarding its monitoring of its implementation of ID.me. For example, while acknowledging that certain groups may encounter difficulties with the verification process, the Department did not capture information on the time it took applicants to resolve those difficulties. Overall, officials indicated that ID.me reduced the time it took applicants to verify their identity as part of the application process. They noted that, prior to ID.me, about 50% of applicants who needed to take additional verification steps had to do so through OSI, which contributed to delays in applicants receiving benefits. However, the Department did not have data or statistics to support the 50% figure or statistics to support the length of time the verification process took for those applicants who had to go through additional verification steps (prior to ID.me) or use the trusted referee process once ID.me was implemented for comparison.

ID.me provides reports to the Department that show cumulative data such as total applicants verified for a period and whether they verified online or via the trusted referee.  According to the cumulative report, for the period February 22, 2021 to March 17, 2022, of the 729,865 applicants who were able to verify their identity through ID.me, 75% (546,843) did so online; the remaining 25% (183,022) of applicants needed to take additional steps to use the trusted referee during that period. The Department did not establish benchmarks or guidelines or capture the necessary data to fully assess whether 25% is an acceptable level of applicants who must take extra steps to use the trusted referee process. Although the Department generally recognized that the online verification rate of about 75% through ID.me is an improvement over its own previous identity verification process, there is no way to evaluate the degree of improvement. Additionally, the Department did not have any statistics on how long the verification process took for those applicants who had to go through additional verification steps (prior to ID.me) or use the trusted referee process once ID.me was implemented. We also note that the Department did not have statistics on the categories or characteristics of applicants who were not able to complete the online process. This is especially notable as even ID.me has acknowledged that certain vulnerable groups, like young, old, less affluent, and recently migrated individuals, including those with LEP, are at a disadvantage when it comes to proving their identity online.

We question how officials can evaluate the effectiveness of their implementation of ID.me as a key control in the UI benefit application process without certain statistics and data. In response to our preliminary findings, Department officials stated that “a formal report is not necessary to ascertain where claimants struggle both with the normal UI process and with ID.me.” They further claimed that “based on weekly reports, they knew at an early stage those customers that struggled with the verification process.” However, officials did not provide statistics or figures on how they knew such information. As noted previously, ID.me reports show cumulative data information such as categories of applicants whose identities were verified or not verified for a period, and whether they verified online or via the trusted referee. It’s unclear how the Department used this information to determine which types of customers had difficulty with the process. The Department further described their “grass roots” efforts to assist customers through phone, email, or other inquiries to its Claimant Advocate Office, but we note that no data, statistics, or other evidence was provided to support these activities.

The Department’s response also described other actions taken, including developing a list or matrix of common scenarios a call center agent may encounter. However, we reviewed this list and found it simply listed common problems and recommended solutions for call center employees to follow. It did not address specific characteristics of either the caller or the difficulty they were having, and no additional information was provided to support how the list of scenarios was developed (e.g., whether it was based on statistical information or anecdotal information from call center staff). Department officials claimed they relied heavily on weekly verification reports early in the implementation of ID.me, but as the percentage of applicants who verify online has stabilized, they focus more on daily reports. These daily lists go to one of the Department’s call centers and are handled by specialized staff. Staff will help applicants verify with ID.me and, once verified, will assist the applicant with getting their claim processed.

The Department’s explanations in its response to our preliminary findings suggested the information it has focused on the tactical or operational (e.g., daily reports, phone calls, emails) rather than broader data or statistical reports to assess the overall implementation of ID.me. Consequently, the Department could not provide statistics, data, or analysis it had used to monitor and make decisions related to its implementation of ID.me. As noted previously, this included no data on the characteristics of those populations that couldn't verify online or the actual improvements in the time it takes to go through extra verification steps. We maintain such information is important and useful for a high-level assessment of patterns or trends to determine whether ID.me is being maximized to ensure all classes and categories of applicants are equally successful in the identity verification process and can access their benefits with the least amount of delay.

## Outdated UI System

As far back as 2010, a national report[5] found that 90% of states relied on legacy mainframe systems operating on older technology and outmoded programming languages such as COBOL, CICS, or VSAM. The report pointed out numerous adverse effects of these outdated systems for UI, including that they are difficult and costly to support because fewer IT staff are skilled in old technology, and they lack the agility necessary to adjust to new laws and the scalability to handle workload surges.

Similarly, in our prior audit report, *Security and Effectiveness of the Department of Labor's Unemployment Insurance System* (2014-S-9), issued February 24, 2015, we commented on the shrinking pool of individuals proficient in the computer languages necessary to keep the Department's mainframe UI system running without interruption. The audit response indicated there was a long-term plan to modernize the Department's UI system and eliminate its dependence on mainframe applications. Most recently, a May 2021 report by the USDOL Inspector General, *COVID-19: States Struggled to Implement CARES Act Unemployment Insurance Programs* (May 2021 USDOL Report), noted previous concerns that states' legacy IT systems would impede the management and oversight of UI benefits.

The Security Policy, originally issued in 2003, defines the responsibilities of all State agencies, including the Department, to ensure a secure and stable IT environment. The Security Policy states that advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis. In addition, in its 2016-17 and 2017-18 Internal Control Summary and Certification documents, the Department identified UI as a high-risk program.

We found the Department did not modernize its existing, outdated UI system prior to the COVID-19 pandemic despite warnings and acknowledgment of the necessity to do so. The inflexibility of the technology on which the UI system is based hindered the Department's implementation of newly legislated programs, and forced officials to make claims processing decisions based on what could and would work within the

[5] National Association of State Workforce Agencies, Center for Employment Security Education and Research, and the Information Technology Support Center: *A National View of UI IT Systems*, July 2010.

existing system parameters and required time frame. Ultimately, this led to benefits being paid from incorrect programs, which later consumed Department resources to identify and correct.

Department officials explained they used a local office code (local code) already in the system to process benefits as a way to leverage the existing coding within the mainframe to swiftly implement a brand-new federal program that had different requirements than traditional UI. In fact, ITS officials noted that the complexity of the UI system made the significant changes needed to respond to the pandemic risky, and the impact of any proposed changes on other critical functions had to be considered. The local code was in place and had been used in the past for emergency payments, such as disaster unemployment assistance. Department officials concluded it would be the only way to process UI benefits under the new temporary programs. Making changes to the mainframe system would be difficult due to a lack of experienced staff. However, the use of the local code led to misclassifications and overpayments because it overrode certain controls in the UI system that limit payments to the maximum allowable amounts. In response, Department officials explained that, at the same time, they were challenged to build new applications that would provide timely information to claimants as well as add capacity to the system. For example, the system, at the onset of the pandemic, did not have the capacity needed to fulfill the number of claims being submitted, nor could it easily be updated to upgrade its capacity. This led to 102 changes to the system that were needed to allow for more transaction processing and 10 other changes to add to the memory and processing power for the UI system. Department officials also cited a lack of experienced and knowledgeable workers to support the mainframe system and work on these tasks.

As shown on page 19, as early as 2010, reports demonstrated the dire condition of state UI systems and the urgent need to modernize them, including our prior 2015 audit report. However, the Department did not issue a request for proposal for a redesigned system until June 2017 – more than 2 years later. Further, it wasn’t until 2019 that a contract was awarded to Tata Consultancy Services Limited to build a new UI system for approximately $57 million. According to officials, work continued on development of the new UI system throughout the pandemic, and they expected it to be available in fall 2023. They also stated that the new system will address the issues with the old mainframe technology that they faced during the pandemic. For example, officials claimed the new UI system will provide easier scaling via the cloud when UI claims surge and easier maintenance because it is based on a more modern infrastructure that won’t rely on specialized, experienced staff.

The absence of a modern, adaptable UI system challenged the Department to make critical decisions to keep up with the demand for UI benefits during COVID-19 and pay claims quickly. These decisions led to misclassification of claims, overpayment of claims, and supplemental spending to maintain the outdated UI system infrastructure while the new system was in development. It also presented obstacles to capturing important information useful for monitoring and analyzing fraudulent claims the Department identified.

**YEAR**

**2010**

**JULY**
A National View of UI IT Systems reports that 90% of states rely on legacy mainframe systems using outmoded programming languages that are difficult and costly to support. Old UI systems are not agile or scalable, meaning states have difficulty implementing changes and scaling up to handle workload surges.

**2013**

**DECEMBER**
DOL's Disaster Recovery Testing of the UI System states that some technical aspects are known to only one person. The knowledge base needs to be expanded via employee cross-training, better documentation, and a defined succession plan for responsibilities.

**2014**

**FEBRUARY - SEPTEMBER**
OSC audit report 2014-S-9 notes that DOL stores all UI data on its mainframe, which was programmed using older programming languages. The pool of individuals proficient in these languages is small.

**DECEMBER**
In response to the draft report, ITS cites both a short-term plan (< 5 years) to hire and train staff in older technologies and a long-term plan (> 5 years) to modernize the UI system and eliminate DOL's dependency on legacy mainframe applications.

**2017**

**JUNE**
In its 2016-17 Internal Control Certification, DOL identifies UI as a high-risk program.

Faced with the pressing problem of maintaining, modifying, and extending an outdated and expensive mainframe-based UI system, DOL issues a request for proposal to design, develop, and implement a new UI system.

**2018**

**JUNE**
In its 2017-18 Internal Control Certification, DOL again identifies UI as a high-risk program.

**2019**

**MAY**
DOL awards Tata Consultancy Services Ltd a $56.6 million contract for the design, development, and implementation of a new UI system.

**2020**

**MARCH**
Congress passes the CARES Act, which provides enhanced UI benefits for those affected by the COVID-19 pandemic.

**APRIL**
Due to the dramatic increase in UI claims, DOL works with vendors to expand system capacity and update UI applications such as cloud services.

**APRIL - SEPTEMBER**
DOL contracts with IBM for $13 million for additional mainframe data entry and coding of claim information into the UI system and application processing services.

**2022**

**PRESENT**
Contractor continues development of new UI system, with implementation expected in fall 2023.

## Questionable Claim Payments

During the pandemic, the Department was tasked with managing an unprecedented volume of claims while still getting payments to those in need of assistance quickly, within the constraints of the existing system. We found that, in order to accomplish this, the Department used a "pay and chase" method for processing State and federal UI benefits during the pandemic. For example, as previously noted, Department officials instructed staff to use the local code to assist with paying benefits. However, among other things, this local code overrides the automated internal controls in place that enforce the 26-week maximum for traditional UI claims. Department officials stated that transactions using this code are reviewed on a sample basis, with emphasis on transactions overridden by new hires. However, using this code allowed claimants to be paid from incorrect program funds and increased the risk that a claimant may be overpaid. It was also another opportunity for inaccurate and unreliable data to make its way into the Department's UI system.

Department officials explained that the local code was in place and used in the past for emergency payments such as disaster unemployment assistance. For example, it was used after Superstorm Sandy in 2012 to assist claimants in getting benefits quickly and ensuring those benefits continued with expanded programs. With this prior experience in hand, we questioned officials why they had not changed or upgraded the system since then to ensure that, in future emergency situations, the local code could be used without jeopardizing the integrity of existing internal controls that prevent payments in excess of the maximum allowable benefits for each program. Department officials responded that the complexity of the UI system made the significant changes needed to add the temporary federal CARES Act programs risky. The impact of any proposed changes on other critical functions had to be considered. Further, there was initial uncertainty about the extent of the impact COVID-19 might have, and when the CARES Act was signed into law on March 27, 2020, Department officials noted they had little time to establish a system to process payments under the new programs. According to Department officials, federal officials stated the new programs would be similar to the program during Superstorm Sandy. Therefore, Department officials concluded that it was best to use the local code. Further, while the Department stopped using the local code in September 2021 when the temporary UI programs expired, as of March 2022, it was still available for use should the need arise to manage emergency situations.

There is some evidence that the Department's decision to use the local code did result in getting payments out faster. The May 2021 USDOL Report shows that New York, despite not having a modernized system, was among the fastest states to pay out benefits from the temporary programs. Yet the speed came at the expense of payments misclassified on the UI system and overpayments to UI claimants because use of the local code overrode the automated internal controls in place that enforce the 26-week maximum for traditional UI claims. Subsequently, the Department needed to expend staff and financial resources to adjust, reclassify, and recover improper payments.

During our initial testing of 53 claimants, selected for various risk factors, we identified 18 claimants who potentially received UI payments in excess of the maximum allowed amount. We then selected another 100 claimants, all of whom appeared to receive UI payments in excess of maximum allowed amounts. We reviewed the detailed claim payments totaling $3,250,044 for the 118 claimants and determined 96 claimants were improperly paid $2,755,141 through the State's traditional UI program instead of the temporary federal CARES Act programs. In addition to payments for our sampled claimants, we identified another $41.2 million in questionable payments made to 8,798 claimants (excluding the 118 in our sample), whose payments appeared to be in excess of the maximum allowed amounts. We question if these claims were correctly paid or if the appropriate funding source (State or federal) was used. We also note that another five of the 118 (4%) were actually overpaid $37,700 because subsequent adjustments caused duplicate payments in these cases.

During the audit, we found the Department had identified, investigated, and corrected the codes on each of the 96 claims in our sample to reflect the appropriate temporary federal CARES Act program. Department officials explained that benefit payments are allocated to the State versus federal accounts via daily and monthly reports to the USDOL, and that any benefit payments that are reclassified to and from State versus federal programs are adjusted on the reports to the federal government as the adjustment occurs. Therefore, there is not an outstanding amount that needs to be recouped from the federal program. However, subsequently, in response to our preliminary findings report, officials instead indicated that the Department identified misclassification issues and adjusted claims on its UI system, but adjustments to federal reports have not occurred. Further, Department officials are waiting for the USDOL to provide guidance on how to resolve the errors. Until the claims are investigated, corrected, and adjusted, they are still incorrectly paid with State funds.

The incorrect payments of claims with traditional UI funds rather than temporary federal CARES Act funds can also affect potential assessments on businesses that are taxed to fund the UI program as well as the accuracy of internal and external reporting. A 2021 OSC report, *Unemployment Insurance Trust Fund: Challenges Ahead* (2021 Comptroller's Report), explains the impact of UI claims during the pandemic on the State's UI trust fund along with the accompanying borrowing and taxes to support it. Until the UI trust fund balance returns to a positive level, employers will continue to make State UI contributions between 2.1% and 9.9%, according to the report. With businesses under pressure from these increased assessments, it's important that payments by the Department are accurate and reflect the correct program funding used to pay claims and do not weigh on the UI trust fund's ability to recover. As previously noted, in July 2022, the Department also assessed an IAS of 0.23% on New York businesses to cover interest owed on its loan from the UI trust fund.

The Department also risks using inaccurate or incomplete information for program processing and reporting purposes. For example, the Department is responsible for identifying and reporting on fraudulent and improper claim payment information to the USDOL for oversight purposes. However, the May 2021 USDOL Report noted that states reported less than expected and unreliable information about fraudulent and overpaid claims in both traditional UI and CARES Act UI programs. If the USDOL does not have accurate information from states, including New York, it cannot make accurate assessments of its programs.

## System Scaling and Staffing

Among other issues, the old mainframe UI system made it difficult for the Department to add additional staff who are knowledgeable in old programming languages as well as system capability and capacity during the pandemic claim surge. Department officials described how the mainframe data is stored in codes to save space. However, experts familiar with this mainframe data are needed to create reports or change applications. Further, mainframe development needs programmers experienced in the older programing languages of Assembler, COBOL, and PL/1, which are less common. As such, it was more difficult to find experienced staff knowledgeable in these languages. Our 2015 audit cited these same concerns, as did the Department's December 2013 *Disaster Recovery Testing of the Unemployment Insurance System*, which stated: "Due to staff unavailability, it became evident during the testing process that some technical aspects are known to only one person. The knowledge base needs to be expanded via: a) employee cross training, b) better documentation, and c) defined succession plan for responsibilities." Consequently, the Department was especially challenged to operate its mainframe-based system during the pandemic surge.

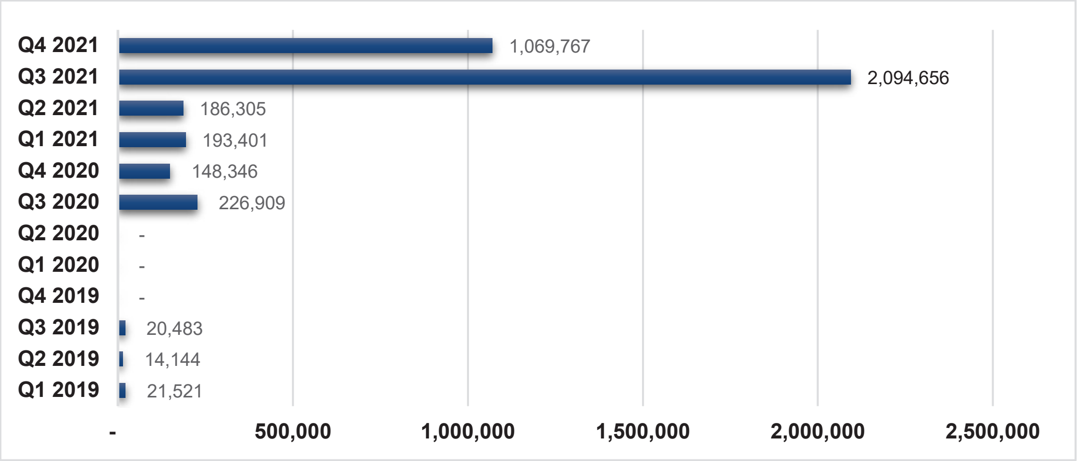
Prior to the COVID-19 pandemic, ITS maintained a contract with IBM for data entry services related to New York State's mainframe systems, including the UI system. During the COVID-19 pandemic, ITS contracted twice with IBM for more than $13 million in additional mainframe data entry and coding of claim information into the UI system and application processing services that covered the period April 2020 to September 2020. Had the Department been using a more modern system that could more easily be supported by Department and ITS staff, this additional cost for specialized services could have potentially been avoided. Department officials disagreed, stating that additional resources were necessary to respond to the surge in the volume of claimants and would have been necessary regardless of the type/capacity of the system being used. While we agree generally that additional staff were necessary due to the claim surge, in this case, the IBM contract required staff with specific skills, including the ability to navigate data entry in COBOL mainframe systems.

In addition to staffing, the Department was also challenged to expand capacity of the mainframe UI system to accommodate the pandemic claim surge. Department officials explained the mainframe-based UI system had a limited capacity. Expanding the number of fields to accommodate the surge in claims took time, and they had to coordinate with ITS to accomplish this. To address this challenge, the Department also worked with Google to create a cloud-based solution for UI applications that fed data into the existing mainframe system. Going forward, Department officials cited the design of the new UI system that will be more agile and better meet the needs of the Department's customers as well as staff.

## Language Information

The Department's outdated UI system also prevented it from capturing sufficient and useful information about languages used by LEP claimants. According to its quarterly reports, the Department saw an increased demand for language interpretation services by LEP UI applicants from 20,483 in the third quarter of 2019 to 2,094,656 in the third quarter of 2021 (10,126%). Figure 2 shows the increased use of language interpretation services from before the pandemic and its peak usage of these services in the third quarter of 2021.

Figure 2 – Demand for Language Interpretation Services, 2019–2021



Note: Quarterly reports were not prepared for fourth quarter 2019 through second quarter 2020.

According to the Standards, information is necessary for an organization to carry out internal control responsibilities to support the achievement of its objectives. Internal communication is the continual, iterative process of obtaining, providing, and sharing necessary information. Further, to comply with Executive Order 26, as amended by Executive Order 26.1, which established New York's Statewide Language Access Policy, the Department prepared a Language Access Plan (Plan) to ensure that LEP individuals have meaningful access to agency services, programs, and activities.

While the Department captures language access information related to UI claims for LEP individuals, it does not do so in a systematic and timely way via the UI system. Instead, the process still relies on a system of notes in LEP claimant communications and quarterly summary reports to track language information rather than track language information in a real-time, systematic manner on the UI system. According to the Department's current Plan, employees who work with the public are instructed to keep track of encounters with LEP individuals and make a note in the individuals' records so future communication can be made in their preferred language. Quarterly, the various divisions and offices within the Department then report this information to the Language Access Coordinator. However, Department officials don't have an easy way to analyze this information to ensure it is in a position to best manage its resources and monitor how it serves LEP users of the UI system. For example, during the COVID-19 pandemic, when the volume of UI claims surged, Department staff or volunteers had to follow up with claimants to verify UI claim information that was submitted. We question how the Department would know to assign follow-up calls to employees or volunteers with the ability to speak the claimant's preferred language without going into the written notes of each individual claim. In response to our preliminary findings report, Department officials agreed it could better capture language information, but noted that its ability to make these improvements is limited by the 45-year-old mainframe-based IT system. However, according to the Department's response, despite the aged system, the Department was able to make significant improvements relative to access for LEP individuals.

## Recommendations

1. Continue the development of the replacement UI system and ensure its timely implementation.
2. Take steps, including collecting and analyzing data related to the identity verification process, to ensure the correct balance between fraudulent identity detection and a streamlined process for those in need of UI benefits.
3. Follow up on the questionable claims identified by our audit to ensure adjustments have been made so they are paid from the proper funding source and overpayments are recovered, as warranted.
4. Develop and implement a process to include specific language access information in the UI system to provide the Department with appropriate, current, complete, accurate, accessible, and timely information on LEP individuals.

## Compliance With ITS Policies

In addition to managing the program portion of UI, the Department must ensure its UI system complies with ITS policies and standards. The Security Policy, originally issued in 2003, defines the responsibilities of all State agencies, including the Department, to ensure a secure and stable IT environment. The Security Policy states that advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

Overall, we found the Department has not taken some fundamental, critical steps established in the Security Policy and the Classification, Encryption, Authentication, and Logging Standards to secure its current UI system and data. For example, we determined the Department did not classify data on its UI system, failed to encrypt certain information, did not enforce strong access controls or authentication rules, and did not have a policy in place to ensure systems logs were monitored. Furthermore, some of its changes to the UI system made in response to the COVID-19 pandemic did not meet all the necessary requirements of the ITS Change Management Process and Policy, intended to ensure the mitigation of risks and minimize disruption to critical services. Collectively, this non-compliance increases the risk for unauthorized access to the UI system and information.

## Lack of Data Classification

As a data owner, it is the Department's responsibility to classify the data in its systems. According to the Classification Standard, information classification is based on three principles of security: confidentiality, integrity, and availability. For each principle, information should be classified as low, moderate, or high based on the potential impact to the Department if events occur that jeopardize the information and/or information system. Each system must then have a set of controls in place commensurate with the classification of any data that is stored on or passes through the system. It is the responsibility of ITS to implement controls and to secure the data appropriately based on the classification by the Department. Information assets must be reviewed and reclassified (if needed) on a recurring basis or immediately when any changes to the individual data elements occur.

As discussed further below, a prior audit of the security of the UI system (2014-S-9) found that the UI data had not been classified as required. During the current audit, the Department's inability to produce requested relevant information raised similar concerns.

We requested data classification information three times between October and December 2021. In December 2021, Department and ITS officials provided a classification for just one UI subsystem. Also, in response to our preliminary findings, Department officials asserted that they had performed all the required remaining classifications; however, they did not provide any evidence that regular classifications had been completed, as required by the Classification Standard.

As mentioned, the Department's compliance with the Classification Standard is not a new issue. Our 2015 audit of the security of the UI system (2014-S-9) similarly found that the UI data had not been classified as required. In response to that audit, ITS officials stated that the Department was aware of its responsibility for making classification and control decisions regarding its data and had made progress with data classification. However, more than 7 years later, the Department has yet to accomplish it. If the Department does not review and classify its information and the data on its systems on an ongoing basis as required, it is unable to ensure that the controls developed to protect the confidentiality, integrity, and availability of its data are appropriate and commensurate with the data's classification. This increases the probability that sensitive data will not have adequate security controls, increasing the risk of sensitive data being compromised. We recommend that the Department take steps to classify the information on its UI system.

## Lack of Compliance With the Encryption Standard

Encryption enhances security and protects electronic data by transforming readable information into unintelligible information, and is an effective tool in mitigating the threat of unauthorized access to data. According to the Encryption Standard, encryption is required for data stores that contain personal, private, or sensitive information. The need for encryption is based on the information's classification, risk assessment results, and its intended use.

On July 14, 2021, we requested the encryption configurations for portions of the Department's UI system. In its January 2022 response to that request – more than 5 months later – Department officials informed us that, based on their understanding of the Encryption Standard, they have sufficient encryption in place to comply with its requirements, but did not provide any evidence to support their claim. Later, after consulting with ITS officials, Department officials provided us with further information. Based upon this information, we reported our findings to Department officials in our preliminary report and, consequently, do not address them in detail in this report due to their confidential nature. However, with no data classification in place, the Department cannot be confident that the correct encryption controls, commensurate with the classification of the data, will be developed. We recommend the Department follow up with ITS to ensure the proper encryption is in place for the UI system where required.

## Weak Access Controls

According to the Security Policy, data owners, such as the Department, are responsible for determining who should have access to protected resources, like computer systems, within their jurisdiction and what those access privileges should be (e.g., read, update). Access is managed by authenticating users often through user IDs and authentication tokens like passwords, key fobs, or biometric means, which must be used to authenticate identity. We determined that the Department did not use recommended methods to grant access to certain newly hired employees, did not comply with certain portions of the Authentication Standard, and did not have a separation of duties among system administrators.

### Practices for Granting System Access

NIST 800-53 requires role-based access control (RBAC) – a policy that enforces access to systems and functions based on defined roles (i.e., job functions). Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization's defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. Additionally, under the Security Policy, information owners, such as the Department, are responsible for determining who should have access to protected resources, like computer systems, and access privileges should be limited only to those necessary to accomplish assigned tasks in accordance with the State entity's missions and business functions (i.e., least privilege).

We determined the Department assigned access privileges based not on defined roles but rather on existing users. In addition, the Department maintains a "Do Not Model" list of employees whose access privileges should not be modeled, rather than using baseline templates for different roles. (The "Do Not Model" list consists of individuals who are deemed to have elevated privileges that should not be given to a new user account.) However, of a judgmental sample of 65 newly hired employees, we determined five were granted access to systems based on individuals included on the "Do Not Model" list. In response to our preliminary findings, Department officials agreed access is modeled on existing users and, in certain cases we identified, on individuals from the "Do Not Model" list. Department officials reviewed the access for the specific cases we identified and pointed out that, for two employees, the individual used to model access was not yet on the "Do Not Model" list at the time access was assigned due to a timing lag. Therefore, they considered access for two of the five employees appropriate. For the five employees we identified, Department officials reviewed their access and determined that it was commensurate with their job responsibilities. Nevertheless, these examples highlight the risks of using a "Do Not Model" list, which requires strict attention to maintenance, keeping it up to date and accounting for timing lags when any changes (i.e., additions and deletions) are made. Although the individuals did not have access above and beyond what was warranted for their job responsibilities, the Department's process for granting access is risky and should be reviewed. Elevated access, especially when inadvertent and undetected, increases the risk that employees could make unauthorized or erroneous changes to systems or data.

## Lack of Authentication Standard Enforcement

The Security Policy states that access to systems must be provided through the use of individually assigned, unique identifiers known as user IDs. Each user ID is associated with an authentication token (e.g., password, key fob, biometric), which must be used to authenticate the identity of the person or system requesting access. The Authentication Standard lists the appropriate authentication tokens that can be used with systems developed or operated by State entities, including the minimum requirements for tokens such as passwords. We determined the Department did not comply with certain requirements in the Authentication Standard. The non-compliance affected 28% of user accounts for a portion of its UI system. Due to their confidential nature, we communicated the details of the non-compliance to Department officials in a separate report and do not address those details here. Strong user ID and password credentials used for authentication are the first line of defense to protect access to a system. Without strong authentication rules that are enforced, there is an increased potential for accounts to be inappropriately accessed by unauthorized individuals.

We note that the Department was not forthcoming with the information necessary for our audit work related to evaluating user access controls. On July 14, 2021, we requested support for compliance with certain Authentication Standard requirements. Department officials initially provided supporting documentation for two of the requirements on August 31, 2021. However, it took them until January 2022 – more than 160 days after our initial request – to provide supporting information for the remaining requirements, resulting in significant delays to the audit.

### Separation of Duties and Lack of Compliance With the Logging Standard

According to the Security Policy, duties and areas of responsibility must be separated where appropriate to reduce the risk of accidental or deliberate system misuse. Whenever separation of duties is not technically feasible, other compensating controls must be implemented, such as monitoring of activities, maintaining audit trails, and supervision by management. In addition, according to the Logging Standard, security logs record data so that systems can be appropriately monitored. This monitoring allows authorized staff to support operations, maintain awareness of security events, and verify compliance. Further, the Logging Standard requires that log data be initially analyzed as close to real time as possible.

Due to their confidential nature, we communicated the details of our findings to Department officials in a separate preliminary report and do not address those details here. Department officials claimed that programs within the UI system contain control and exception reports, which are distributed to program staff for review and follow-up. They also stated that they monitor system activity and work closely with ITS development and system maintenance staff to review processing, follow up on, and resolve any issues that arise. However, despite our repeated requests, as of February 2022, they did not provide any evidence of the specific logging and review processes they described.

Department officials also asserted that a significant amount of logging takes place related to the UI system. The volume of logging notwithstanding, we note that the log data that the Department described is recorded in a machine-readable format and is not readily usable for monitoring purposes. Furthermore, merely capturing information in logs is not enough; without a process for also reviewing it, the value of the log information will not be fully realized.

## Compliance With System Change Requirements

During the COVID-19 pandemic, the Department and ITS were forced to make system and process changes to keep up with the increased volume of UI claimants and claims. These changes included implementing new systems and updating existing systems in order to meet new program needs and volume. The Information Security Controls Standard requires a formal change management procedure, formal test plans, and documented results for any changes to State computer systems. According to the ITS Change Management Process and Policy, when changing or modifying computer systems, required steps include creating and recording a change request, approving the requested changes, testing the changes, and reviewing and evaluating the changes. Bypassing the defined steps and processes outlined in the ITS Change Management Process and Policy increases the likelihood of incorrect changes or changes that do not function as initially intended.

We determined that, for certain changes to the UI system, the Department did not perform or provide evidence that it implemented all of the steps required in the ITS Change Management Process and Policy. For a judgmental sample of 12 changes made to its UI system, four changes did not have evidence of approval of the change request and six did not have evidence of testing. In addition, the Department did not provide evidence that any of the 12 changes underwent a post-implementation review. A post-implementation review determines if the change and its implementation project were successful and identifies opportunities for improvement. While not always required, it is a critical piece of the change management process and may have been of benefit to the Department as, according to documentation provided by the Department, three of the changes led to conflicts within the UI system.

As with our review of Authentication Standard requirements, the Department introduced a delay of nearly a year in responding to our repeated requests for information necessary to conduct our review of its compliance with system change requirements. In our initial request on March 18, 2021, we asked the Department for a listing of all changes to the UI system. The Department did not provide a sufficient list from which to pull a sample until September 2021. After reviewing the information provided, on October 28, 2021, we requested documentation to support a sample of 12 changes made to its UI system. The sample of changes included the implementation of ID.me, the Google Web Graphical User Interface, OKTA implementation for authentication, and an upgrade to the UI Data Warehouse, which were important to support the evolving UI claims process. In January 2022, the Department provided information for nine of the 12 changes. In February 2022, the Department finally provided information on the remaining three changes.

## Lack of Timely Responses to Requests

In order to meet government auditing standards, auditors require unfettered access to information relevant to the audit. To accomplish our audit objective, we sought to evaluate the Department’s oversight and management of its UI system and test its adherence to selected requirements in ITS Policies and Standards. As discussed in this report, the Department took excessive time – often more than 160 days, and in one case more than 180 days – to provide the information necessary for us to assess its compliance with applicable IT standards and in other instances failed to provide it altogether.

In response to our preliminary findings, the Department pointed out that Department and ITS officials participated with OSC in biweekly status meetings. While this is true, it is also true that we used those meetings to repeatedly follow up on requested information that had yet to be provided – and that should have been readily available. In the absence of requested information, we used these meetings to solicit the needed information. We noted that Department officials seemed unfamiliar with their basic security controls, as they could not tell us about or demonstrate their logging system or the change management process they had in place for the many changes to the system during the pandemic. In other instances, Department officials did not provide supporting documentation related to fraud prevention and savings of $36 billion that it had reported publicly. These actions ultimately limited the scope and depth of our audit conclusions.

Further, as mentioned, the information we requested should have been readily available. That the information was unavailable or not easily retrievable causes us to question the Department's ability to ensure that the confidentiality, integrity, and availability of its information is protected and maintained in a secure and stable IT environment.

## Recommendations

5. Ensure the current and new UI system and data comply with provisions of the Security Policy, the Classification, Authentication, Encryption, and Logging Standards, as well as the Change Management Process and Policy by:

   - Performing a data classification for the systems and data related to the UI process.
   - Ensuring encryption has been employed where necessary on the UI system.
   - Reviewing and modifying as necessary the procedures for granting system access.
   - Separating duties for administrators of UI applications or implementing appropriate compensating controls.
   - Establishing a formal log monitoring and review process to support operations, maintain awareness of security events, and verify compliance.
   - Ensuring changes to the UI system are fully documented.

6. Improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

# Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether the Department has taken appropriate steps to oversee and manage the UI system and to comply with selected portions of the NYS Information Security Policy and Standards. The audit covered the period from January 2020 to March 2022.

To accomplish our objective and assess related internal controls, we reviewed relevant laws, regulations, policies, and procedures related to the UI programs. We interviewed both Department and USDOL officials. Due to the COVID-19 pandemic, we were limited in our ability to visit the Department's office in person and so conducted meetings virtually. In our professional judgment, this approach does not constitute a scope impairment. Additionally, we reviewed guidance provided by the USDOL related to the pandemic assistance programs. We also reviewed public reports issued by the USDOL and OSC regarding UI, as well as information on language translation services from the Department. We reviewed certain contract information including portions of ITS contracts for mainframe services related to the UI system and the Department's contract for identity verification services. We determined the data was sufficiently reliable for the purposes of our audit work.

To assess whether the Department took appropriate steps to oversee and manage the UI system, we obtained and analyzed over 7.4 million claim records totaling $38.7 billion. Initially, we judgmentally selected records for 80 claimants for review.  We subsequently determined the Department had already identified and addressed risks associated with 25 of the claimants in our sample, and two others were duplicates. Consequently, we excluded them from our sample and reviewed supporting documentation for the remaining 53 claimants (80 - 25 - 2). Our judgments for selecting the claimants whose records we reviewed included those with risks such as highest payouts, duplicate addresses, out-of-state addresses, and duplicate Social Security numbers, and the employee who processed the claim. Based on the results of our initial review, we judgmentally selected an additional 100 claimants for further review of payment accuracy. Our judgments for the additional sample included the particular UI program the claimant's benefits were paid from and the amount by which a claimant's payments exceeded the maximum UI program benefit. We excluded claims that were previously identified by the Department as being fraudulent.

To assess compliance with applicable IT standards, we reviewed relevant ITS system security policies applicable to State agencies such as the Department, along with industry standards issued by NIST. We met with Department and ITS personnel to gain an understanding of their processes for implementing certain controls over systems. We communicated electronically with Department and ITS officials to inquire about and understand the status of certain controls related to the UI system. We performed walk-throughs via WebEx to observe certain system controls and reviewed documentation such as screenshots of system settings to verify controls were in place. We also tested a judgmental sample of 65 (out of 824) newly hired employees to assess whether they were granted appropriate access privileges to the UI system. The judgments for our sample included selecting titles filled by temporary and/or hourly employees with access to sensitive data, as well as the timing of when they were hired during our audit period. In addition, we selected a judgmental sample of 12 (out of 3,314) system changes that occurred during our audit period. We excluded those changes that were canceled or involved hardware changes not related to program functionality. From the remaining 3,254 changes, we judgmentally selected 12 changes for further review based on judgments including whether the change modified the existing program, supported a new program, or added additional control elements that did not exist prior to the change in question. Our sample results only apply to the sampled items, and we cannot and do not project the results of our samples in our audit.

# Statutory Requirements

## Authority

The audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

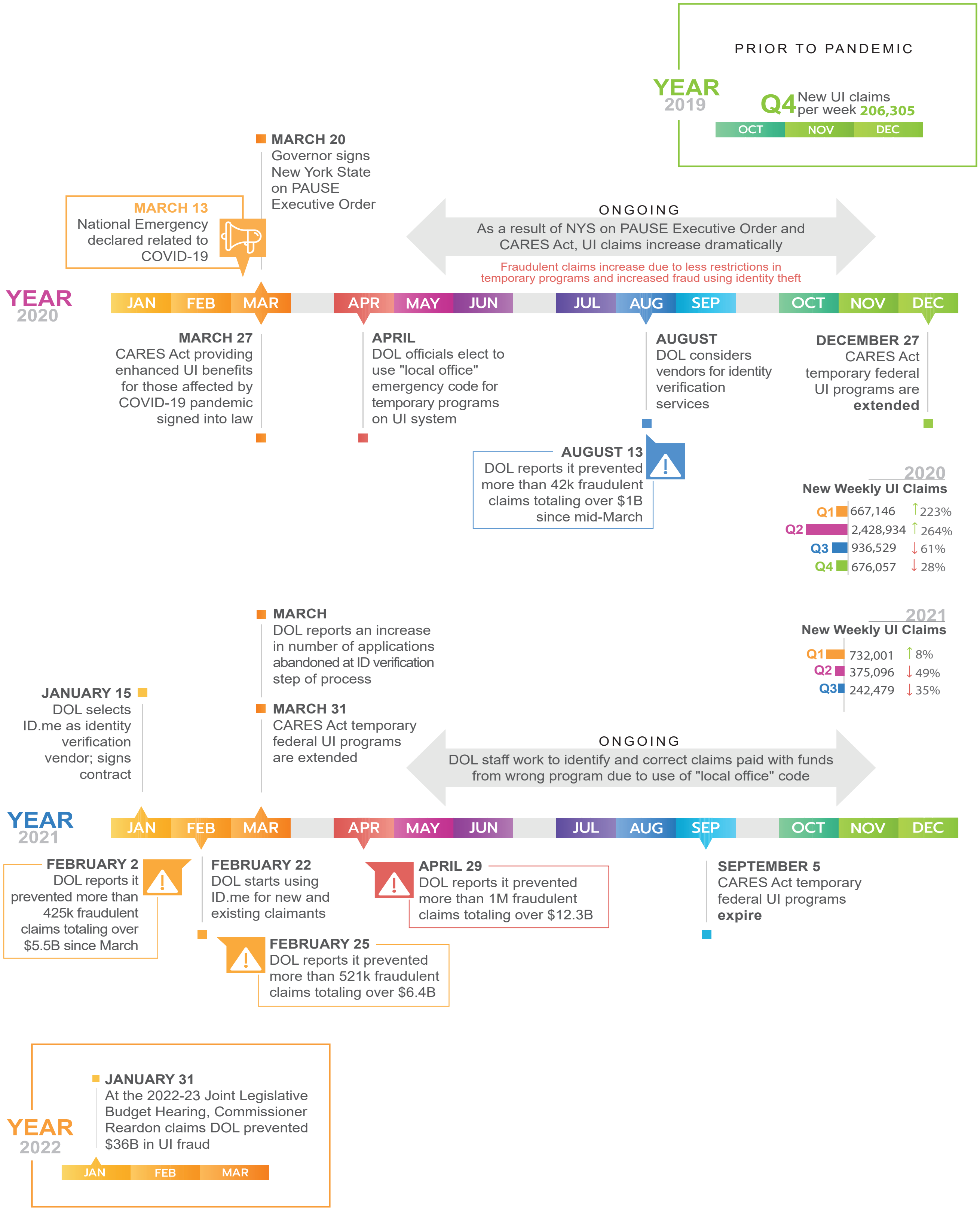
In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. These duties could be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of the Department's controls and management of the UI system.

## Reporting Requirements

We provided a draft copy of this report to Department officials for their review and formal comment. We considered their comments in preparing this final report and have included them in their entirety at the end of it. In their response, Department officials generally agreed with our audit conclusions and recommendations. Our State Comptroller's Comment addressing certain remarks is embedded within the Department's response.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Department of Labor shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

# Exhibit



PRIOR TO PANDEMIC

YEAR 2019

Q4 New UI claims per week **206,305**

YEAR 2020

**MARCH 13**
National Emergency declared related to COVID-19

**MARCH 20**
Governor signs New York State on PAUSE Executive Order

**MARCH 27**
CARES Act providing enhanced UI benefits for those affected by COVID-19 pandemic signed into law

**APRIL**
DOL officials elect to use "local office" emergency code for temporary programs on UI system

ONGOING
As a result of NYS on PAUSE Executive Order and CARES Act, UI claims increase dramatically

Fraudulent claims increase due to less restrictions in temporary programs and increased fraud using identity theft

**AUGUST**
DOL considers vendors for identity verification services

**AUGUST 13**
DOL reports it prevented more than 42k fraudulent claims totaling over $1B since mid-March

**DECEMBER 27**
CARES Act temporary federal UI programs are **extended**

2020
**New Weekly UI Claims**

| | | |
|---|---|---|
| Q1 | 667,146 | ↑223% |
| Q2 | 2,428,934 | ↑264% |
| Q3 | 936,529 | ↓61% |
| Q4 | 676,057 | ↓28% |

YEAR 2021

**JANUARY 15**
DOL selects ID.me as identity verification vendor; signs contract

**MARCH**
DOL reports an increase in number of applications abandoned at ID verification step of process

**MARCH 31**
CARES Act temporary federal UI programs are extended

2021
**New Weekly UI Claims**

| | | |
|---|---|---|
| Q1 | 732,001 | ↑8% |
| Q2 | 375,096 | ↓49% |
| Q3 | 242,479 | ↓35% |

ONGOING
DOL staff work to identify and correct claims paid with funds from wrong program due to use of "local office" code

**FEBRUARY 2**
DOL reports it prevented more than 425k fraudulent claims totaling over $5.5B since March

**FEBRUARY 22**
DOL starts using ID.me for new and existing claimants

**FEBRUARY 25**
DOL reports it prevented more than 521k fraudulent claims totaling over $6.4B

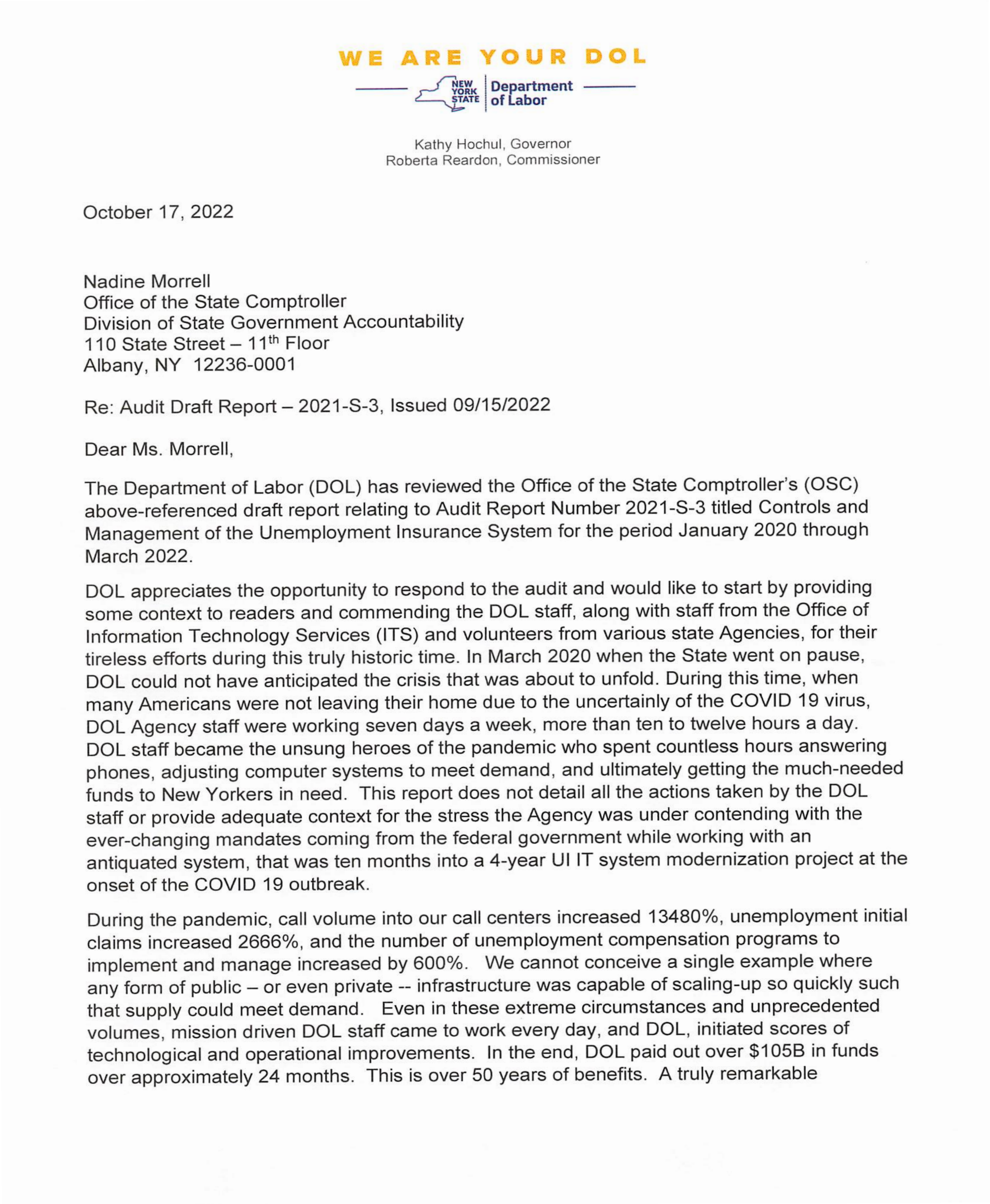
**APRIL 29**
DOL reports it prevented more than 1M fraudulent claims totaling over $12.3B

**SEPTEMBER 5**
CARES Act temporary federal UI programs **expire**

YEAR 2022

**JANUARY 31**
At the 2022-23 Joint Legislative Budget Hearing, Commissioner Reardon claims DOL prevented $36B in UI fraud

# Agency Comments and State Comptroller's Comment



WE ARE YOUR DOL

NEW YORK STATE | Department of Labor

Kathy Hochul, Governor
Roberta Reardon, Commissioner

October 17, 2022

Nadine Morrell
Office of the State Comptroller
Division of State Government Accountability
110 State Street – 11th Floor
Albany, NY 12236-0001

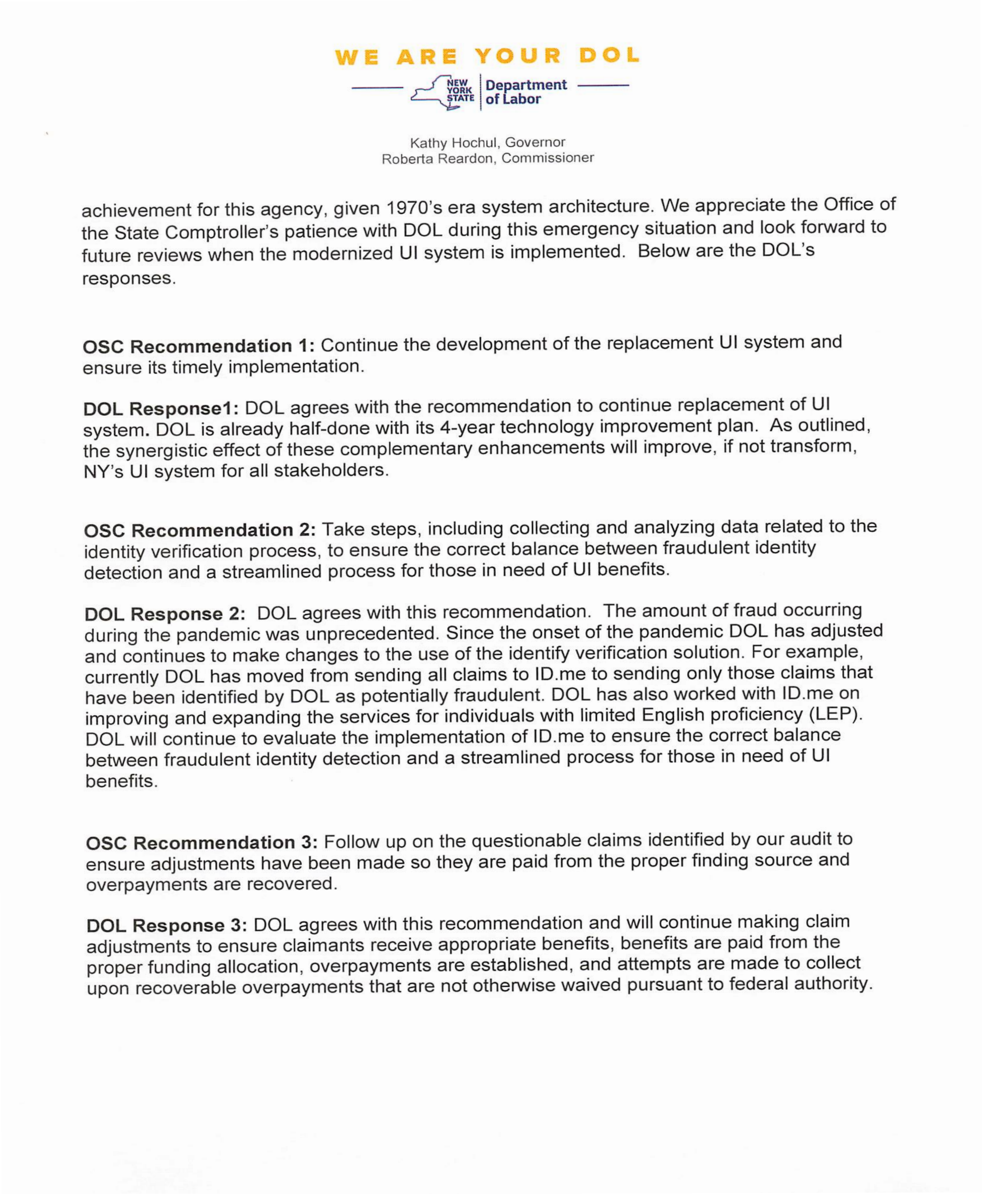
Re: Audit Draft Report – 2021-S-3, Issued 09/15/2022

Dear Ms. Morrell,

The Department of Labor (DOL) has reviewed the Office of the State Comptroller's (OSC) above-referenced draft report relating to Audit Report Number 2021-S-3 titled Controls and Management of the Unemployment Insurance System for the period January 2020 through March 2022.

DOL appreciates the opportunity to respond to the audit and would like to start by providing some context to readers and commending the DOL staff, along with staff from the Office of Information Technology Services (ITS) and volunteers from various state Agencies, for their tireless efforts during this truly historic time. In March 2020 when the State went on pause, DOL could not have anticipated the crisis that was about to unfold. During this time, when many Americans were not leaving their home due to the uncertainly of the COVID 19 virus, DOL Agency staff were working seven days a week, more than ten to twelve hours a day. DOL staff became the unsung heroes of the pandemic who spent countless hours answering phones, adjusting computer systems to meet demand, and ultimately getting the much-needed funds to New Yorkers in need. This report does not detail all the actions taken by the DOL staff or provide adequate context for the stress the Agency was under contending with the ever-changing mandates coming from the federal government while working with an antiquated system, that was ten months into a 4-year UI IT system modernization project at the onset of the COVID 19 outbreak.

During the pandemic, call volume into our call centers increased 13480%, unemployment initial claims increased 2666%, and the number of unemployment compensation programs to implement and manage increased by 600%. We cannot conceive a single example where any form of public – or even private -- infrastructure was capable of scaling-up so quickly such that supply could meet demand. Even in these extreme circumstances and unprecedented volumes, mission driven DOL staff came to work every day, and DOL, initiated scores of technological and operational improvements. In the end, DOL paid out over $105B in funds over approximately 24 months. This is over 50 years of benefits. A truly remarkable



achievement for this agency, given 1970's era system architecture. We appreciate the Office of the State Comptroller's patience with DOL during this emergency situation and look forward to future reviews when the modernized UI system is implemented. Below are the DOL's responses.

**OSC Recommendation 1:** Continue the development of the replacement UI system and ensure its timely implementation.

**DOL Response1:** DOL agrees with the recommendation to continue replacement of UI system. DOL is already half-done with its 4-year technology improvement plan. As outlined, the synergistic effect of these complementary enhancements will improve, if not transform, NY's UI system for all stakeholders.

**OSC Recommendation 2:** Take steps, including collecting and analyzing data related to the identity verification process, to ensure the correct balance between fraudulent identity detection and a streamlined process for those in need of UI benefits.

**DOL Response 2:** DOL agrees with this recommendation. The amount of fraud occurring during the pandemic was unprecedented. Since the onset of the pandemic DOL has adjusted and continues to make changes to the use of the identify verification solution. For example, currently DOL has moved from sending all claims to ID.me to sending only those claims that have been identified by DOL as potentially fraudulent. DOL has also worked with ID.me on improving and expanding the services for individuals with limited English proficiency (LEP). DOL will continue to evaluate the implementation of ID.me to ensure the correct balance between fraudulent identity detection and a streamlined process for those in need of UI benefits.

**OSC Recommendation 3:** Follow up on the questionable claims identified by our audit to ensure adjustments have been made so they are paid from the proper finding source and overpayments are recovered.

**DOL Response 3:** DOL agrees with this recommendation and will continue making claim adjustments to ensure claimants receive appropriate benefits, benefits are paid from the proper funding allocation, overpayments are established, and attempts are made to collect upon recoverable overpayments that are not otherwise waived pursuant to federal authority.

**OSC Recommendation 4:** Develop and implement a process to include specific language access information in the UI system to provide the DOL with appropriate, complete, accurate, accessible, and timely information on LEP individuals.

**DOL Response 4:** DOL agrees with this recommendation. As previously mentioned, DOL is in the process of modernizing its unemployment insurance system. Among other improvements, the new system will allow for more robust data analytics, including LEP data, to promote the goals and objectives associated with the recommendation. Additionally, DOL is seeking a multi-million-dollar grant from the United States Department of Labor – known as an equity grant – that would enhance the inclusivity of New York's UI system for all New Yorkers. The system is expected to go live late 2023.

**OSC Recommendation 5:** Ensure the current and new UI system and data comply with the provisions of the Security Policy, the Classification, Authentication, Encryption, and Logging Standards, as well as the Change Management Process and Policy by:

- Performing a data classification for the systems and data related to the UI process.
- Ensuring encryption has been employed where necessary on the UI system
- Reviewing and modifying as necessary the procedures for granting access.
- Separating duties for administrators of UI applications or implementing appropriate compensating controls
- Establishing formal log monitoring and review process to support operations, maintain awareness of security events, and verify compliance.
- Ensuring changes to the UI system are fully documented.

**DOL Response 5:** DOL agrees with this recommendation. DOL will continue to work with its partners at ITS to ensure compliance with the provisions of the Security Policy, the Classification, Authentication, Encryption, and Logging Standards, as well as the Change Management Process and Policy.

**OSC Recommendation 6:** Improve timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

**DOL Response 6:** DOL agrees with the need for transparent and accountable agency operations. It should be noted that the report fails to consider the competing priorities that ITS and DOL were managing at the time of fieldwork for this audit. All resources were allocated to pandemic efforts. As indicated in the preliminary response, while DOL was tackling a significant increase in claim volume, and both DOL and ITS were managing several concurrent audit requests and systems upgrades, in an effort to ensure responsiveness and cooperation with this audit, both DOL and ITS participated in biweekly status meetings with OSC. During these meetings all requested items were reviewed and questions about the status of outstanding requests were followed up on. At no point did OSC raise any concerns about the timeliness of information being provided. It wasn't until a preliminary draft report was issued, that a concern with delays and the number of days OSC was waiting for specific items was communicated. To improve cooperation with state oversight inquiries going forward, DOL recommends OSC participate in open transparent communication about expectations of timeliness with requested items in weekly status meetings, rather than waiting to issue draft reports with delinquent status. The time lags experienced during this audit were due to the emergency situation DOL and ITS were operating in throughout the course of the audit. Providing clearer communication during status meeting about OSC's expectations for timely responses would have enabled DOL and ITS to balance competing priorities with available resources to both meet the needs of our customers and OSC.

**State Comptroller's Comment –** The Department is incorrect in its assertion. During a meeting in May 2021, long before the preliminary report was issued, we expressed our concerns to Department officials about the length of time it was taking them to provide requested information. It was at this meeting that OSC and the Department agreed to hold the biweekly status meetings the Department references in its response. We also note that these meetings were often the forum for our repeated follow-up on requested information that was still outstanding. As discussed in this report, the Department took excessive time – often more than 5 months, and in one case more than 6 months – to provide the information. Still, we are pleased Department officials agree with the need for transparent and accountable agency operations, and we look forward to their cooperation during future audits.

If you have any comments, please contact Erin Murphy, Director Internal Audit, (518) 457-9076.

Sincerely,

Susan Filburn
Deputy Commissioner Employment Security

Cc: Scott Melvin
Lars Thompson
Stephen Geskey
Jacqueline Kagan
Erin Murphy

# Contributors to Report

## Executive Team

**Andrea C. Miller** - *Executive Deputy Comptroller*

**Tina Kim** - *Deputy Comptroller*

**Ken Shulman** - *Assistant Comptroller*

## Audit Team

**Nadine Morrell**, CIA, CISM - *Audit Director*

**Cynthia Herubin**, CIA, CGAP - *Audit Manager*

**Brian Krawiecki**, CIA - *Audit Supervisor*

**Justin Dasenbrock**, ITIL - *IT Audit Supervisor*

**Richard Podagrosi** - *Examiner-in-Charge*

**Nicole Cappiello** - *Senior Examiner*

**Jason Getman**, CPA, CCSK - *Senior Examiner*

**Marisa DeMania** - *Senior Examiner*

**Mary McCoy** - *Supervising Editor*

**Contact Information**
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller
For more audits or information, please visit: www.osc.state.ny.us/audits/index.htm