incode

Strengthening Call Center Operations with Identity Verification: A Case Study

Introduction

Fraud in call center interactions poses a growing threat to organizations across various sectors, including government agencies. With the increasing sophistication of fraudsters leveraging stolen personal data, traditional methods for verifying identities, such as password-based authentication, are becoming insufficient.

This paper explores a call center use case, demonstrating how identity verification (IDV) technology can bolster security, improve operational efficiency, and reduce costs. Drawing insights from the implementation of the Georgia Department of Driver Services (DDS), this paper highlights how Secretaries or State and similar agencies can implement identity verification strategies to enhance security and service delivery.

The fraud landscape in call center interactions

In an era where digital commerce dominates, consumers still rely on call centers for timely and trustworthy customer service. However, a TransUnion report[1] highlights that call centers are becoming an increasingly attractive target for fraudsters, creating a challenging balance between providing efficient service and ensuring account security.

The report found that **more than half of respondents observed a rise in fraud attacks on call centers**, with financial industry respondents experiencing an even sharper increase—**90 percent reported some level of attack growth**, and **20 percent noted an 80 percent rise since 2021**.[2]

To combat these threats, the report underscores the importance of early fraud detection before a caller reaches an agent. Strengthening pre-answer risk assessments and

---

[1] TransUnion. (2024). *Omnichannel fraud report*. TransUnion. https://www.transunion.com/report/omnichannel-fraud-report

[2] Destination CRM. (2024, January 2). *Call center fraud on the rise*. Destination CRM. https://www.destinationcrm.com/Articles/CRM-News/CRM-Featured-Articles/Call-Center-Fraud-on-the-Rise-161397.aspx.

integrating caller verification technologies can significantly reduce fraud risk, allowing agents to focus on genuine customer needs rather than vetting suspicious callers.

On the other hand, recent studies[3] highlight the increasing risk of insider fraud within call centers, particularly as remote work environments continue to expand. Traditional Security Information and Event Management (SIEM) systems, which rely on rule-based alerts for external threats, have proven insufficient in detecting novel fraud scenarios, insider threats, cyber fraud, or data theft.

Social engineering tactics and stolen personal information enable attackers to pose as legitimate individuals, manipulating agents into resetting credentials or granting unauthorized access to sensitive accounts. Recent studies reveal:

- **Password fraud trends:** A significant portion of call center fraud involves exploiting password recovery processes.
- **Social engineering impact:** Call center agents often lack the tools to differentiate between genuine and fraudulent requests, leaving them vulnerable to manipulation.
- **Cost implications:** Fraudulent interactions increase operational costs, compromise security, and erode public trust.

Georgia DDS: A Case Study

The challenge

The Georgia DDS faced escalating fraud in its online Change of Address (COA) and password reset processes. Hackers were attempting to exploit compromised personal data to bypass traditional security measures, forcing DDS to suspend online COA services temporarily as a precaution. This decision led to increased reliance on call centers, overburdening agents already managing an average of 800 daily calls. The additional volume and extended call times negatively impacted operational efficiency and customer satisfaction.

---

[3] Cardoso, N. A. M. L. (2021). *User behavior analytics in the contact center: Insider threat assessment and fraud detection* [Master's thesis, University of Coimbra]. Talkdesk. https://estudogeral.uc.pt/handle/10316/96092

The goals

To address these challenges, DDS sought to implement a solution that was:

1. Remote, self-service, and accessible 24/7,
2. Secure, ensuring that only legitimate users can access services,
3. Fair, equitable and non-bias in results across all demographic groups, and
4. Consent-based and user-friendly to encourage adoption.

The solution: Biometric Identity Verification

A biometric identity verification system enhances security by using **facial comparison** combined with **liveness detection** to ensure that only the true credential holder can perform a service request. Unlike traditional methods that rely solely on passwords or security questions, **biometric IDV verifies identity through AI-driven biometric proofing**, minimizing the risk of impersonation or fraud.

DDS deployed a biometric IDV solution aligned with NIST 800-63 IAL2 standards. The identity verification process requires the end user to first consent to the verification process and then submit an image of their state-issued credential (Driver's License or ID), along with a selfie.

The solution authenticates the credential (Document Authentication), determines the person submitting is a live human (Liveness Detection), and performs a biometric comparison of the selfie image to the driver's license image on record at the DDS (Facial Comparison/image comparison).

This opt-in, contactless system provided:

- **High assurance:** Verified that the actual credential holder was performing the request.
- **Seamless user experience:** Enabled remote, secure identity proofing without compromising user convenience.
- **Operational efficiency:** Automated processes and reduced manual intervention.

The Role of Face Liveness Detection

At the core of this solution is Face Liveness Detection, which combines facial comparison, biometric authentication, and liveness detection to ensure that the person attempting

verification is real and present. Liveness Detection is a machine learning-powered technology that works alongside facial comparison, document processing, validation, proof of address, and other identity verification methods. Liveness detection answers the fundamental question for preventing presentation attacks: "Is there a live person in front of the camera?"

Liveness detection plays a crucial role in preventing fraud by distinguishing real users from spoofed or manipulated identities, particularly by blocking injection attacks. This particular solution provides passive liveness detection, which offers a frictionless user experience by eliminating the need for user actions, such as head movements or specific gestures. Advanced solutions like this offer enhanced functionality to combat emerging fraud vectors such as AI injection and digital spoofs.

Ensuring fairness and reducing bias

One important solution consideration for GA DDS is that any biometric solution must perform well across all demographic groups, demonstrating minimal bias. This was a key requirement and was satisfied by the National Institute of Standards and Technology (NIST) Facial Comparison bias testing results for the chosen vendor. Two factors contributing to minimal bias in identity verification are limiting the biometric comparison to a single image in a 1:1 comparison and machine learning models built on large and diverse image data sets. The GA DDS solution relies on these two important factors to maximize accuracy and eliminate bias.

Solution Implementation and Results

In late January 2024, after completing functional and end-to-end testing, the State of Georgia contracted the Underwriters Laboratory (UL) to conduct its own Presentation Attack Detection (PAD) levels 1 and 2 testing on the solution. This testing, performed by a qualified and independent body, ensured the solution did not introduce unacceptable fraud risks. The ISO-30107 compliant testing by UL resulted in zero successful attacks against the solution’s passive liveness technology.

Following the successful UL testing, the Georgia Department of Driver Services (DDS) implemented the solution for online address changes. After closely monitoring system activity, DDS concluded that the solution effectively eliminated fraudulent requests in this use case.

In the first 120 days, 268,030 high-risk address change requests were automated using the new solution. These requests, which would have otherwise required processing by DDS call center agents, translated to savings of 1,072,120 minutes of labor—equivalent to 17,869 labor hours or approximately 25 full-time employees (FTEs) per year.[4] According to studies by the Gartner Group, between 20% and 50% of all help desk calls are related to password resets, with each reset typically taking between 2-30 minutes to resolve. While this estimate is based on industry benchmarks, actual savings for GA DDS are likely significant, as the reduction in manual processing frees up resources for higher-value tasks.

Encouraged by the success of the address change use case, DDS extended the solution to customer password resets. This implementation was completed in just three weeks, well ahead of the originally planned eight-week timeline.

According to Forrester Research, the average cost of a password reset call to a call center is approximately $70 per incident.[5] Given that GA DDS processed 4,500 password resets in the first month of implementation, we can estimate a cost savings of over $300,000 in that short period. While this estimate is based on industry norms, it highlights the significant financial impact of identity verification. While actual savings have yet to be calculated, it is evident that cost savings from this use case alone far exceed the cost of implementing the solution.

Results

The GA DDS implementation delivered significant outcomes:

1. **Fraud mitigation:** To date, nearly 400,000 address changes have been processed with 98% accuracy and no detectable fraud.
2. **Operational improvements:** Expanded to password resets, reducing call center volume by 10,000 calls within two months.
3. **Cost savings:** Lowered the opportunity cost by reallocating agents to higher-value tasks, enhancing productivity.

---

[4] **Author Unknown.** (2024). *Password reset calls are costing your org big money.* BleepingComputer. https://www.bleepingcomputer.com/news/security/password-reset-calls-are-costing-your-org-big-money/

[5] **Forrester Research.** (2024). *Best practices: Selecting, deploying, and managing enterprise password managers.* Forrester. https://www.forrester.com/report/best-practices-selecting-deploying-and-managing-enterprise-password-managers/RES139333

Key Benefits for Secretaries of State and Agencies

1. **Enhanced Security:** Biometric IDV ensures the highest level of identity assurance, minimizing risks associated with traditional methods.
2. **Cost Efficiency:** Reduced call center workloads translate into significant cost savings, both in fraud prevention and operational expenses.
3. **Resource Optimization:** Freed-up agents can focus on complex, high-value interactions rather than routine identity verifications.
4. **Scalability and Accessibility:** A 24/7 self-service solution meets the growing demands of constituents while maintaining service quality.

Broader applications

Beyond DDS, similar solutions are generating successful results for other agencies. Securing remote and online agency transactions, such as business services and voter registration, and verifying identity for ballot cure are relevant examples for Secretaries of State.

Conclusion

Fraud in call center interactions is a pressing challenge that demands innovative solutions. The Georgia DDS case study illustrates the effectiveness of biometric identity verification in addressing these challenges, offering a blueprint for Secretaries of State and similar agencies. By strengthening security, reducing costs, and optimizing resources, identity verification technology empowers government entities to better serve their constituents while safeguarding sensitive information.

For more information please contact:

Mark Hamilton, Senior Account Executive - State & Local

Phone*: 817.501.8568*

Email*: mark.hamilton@incode.com*