

# 2023 Global Survey: State of Intelligent Authentication and Contact Center Security



opusresearch

April 2023

**Matt Smallman** | Director, SymNex Consulting

**Dan Miller** | Lead Analyst & Founder, Opus Research

**Derek Top** | Research Director, Opus Research

**Peter Headrick** | Managing Director, Opus Research

Opus Research, Inc., 893 Hague Ave., Saint Paul, MN 55104

[www.opusresearch.net](http://www.opusresearch.net)

Published April 2023 © Opus Research, Inc. All rights reserved.



➤ **2023 Global Survey:  
State of Intelligent Authentication  
and Contact Center Security**

## Contents

---

Executive Summary . . . . .	2
Introduction and Methodology. . . . .	3
Heightened Demands on the Contact Center . . . . .	4
Security Issues Exacerbate Longstanding Efficiency Challenges . . . . .	5
Core Platforms Stabilizing in Cloud Migration . . . . .	6
Reality Check: Focus on the Current State of ID&V . . . . .	7
Authenticating Callers: Continued Reliance on Knowledge Questions . . . . .	8
Unrealized Potential of Modern Authentication Methods . . . . .	9
Conclusions . . . . .	10

---

### Table of Figures

Figure 1: Expectations for Increase in Call Volume, Complexity, and Duration . . . . .	4
Figure 2: Expectations for Increase in Calls Related Authentication, Fraud & Security . . . . .	5
Figure 3: Shifting Concerns about Security, Usability & Efficiency . . . . .	5
Figure 4: Percentage of Calls Attempting Automated Authentication & Identification . . . . .	6
Figure 5: Current State of Telephony Infrastructure . . . . .	7
Figure 6: Expectations Moving to the Cloud . . . . .	7
Figure 7: Primary Method for Caller Identification . . . . .	8
Figure 8: Current State of Primary Caller Identification Methods . . . . .	8
Figure 9: Primary Method for Caller Authentication . . . . .	9
Figure 10: Current State of Primary Caller Authentication Methods . . . . .	9
Figure 11: Potential Opportunity for Modern Security Methods . . . . .	10

---



## Executive Summary

Contact centers have long been a go-to attack surface for fraudsters seeking access to personal information or sign-in credentials from customers at banks, financial institutions, retailers, healthcare providers and elsewhere. Growing use of digital channels and mobile apps has changed the nature and complexity of caller authentication in ways that deserve further investigation.

To learn more about enterprise anticipation, expectation and preparation for changing usage patterns and modern authentication requirements Opus Research joined with SymNex Consulting to survey 250 executives decisionmakers involved with their companies' deployment of technologies for customer authentication.

### **A summary of our findings include:**

- Call volume (63%) and call complexity (70%) is expected to increase significantly in coming years as indicated by survey respondents.
- Calls related to problems with security, fraud and authentication are also expected to grow (70%), as well as increases in fraud associated with the contact center (63%).
- After a couple of years of super-normal growth, the rate at which enterprises are migrating contact center resources “to the cloud” is stabilizing with only 10% of respondents expecting significant increases to the cloud this year.
- Tensions remain in efforts to balance customer convenience and agent efficiency with requirements for “strong” security.
- There is growing but modest awareness of “modern” identification and authentication processes and procedure, with just 22% of organizations are deploying modern authentication and fraud prevention procedures.
- Employing automated authentication before reaching an agent is a missed opportunity.



## Introduction and Methodology

Opus Research recently conducted an executive survey to understand technologies enterprises employ for customer authentication, security, and fraud prevention. In particular, the survey sought to understand how these approaches have changed since our last survey, conducted in 2021.

The global survey covered 250 decision-makers (Director, VP, C-level, department head) from organizations with more than \$250 million USD in revenue. Half of the respondents were from North America, and the other half were from the UK and Europe (125 respondents each). In total, respondents were responsible for almost 400 million calls per annum and more than 500,000 full-time equivalent agents. The survey targeted seven vertical industries:

- **Banking and Financial Services**
- **Government Services**
- **Telecom**
- **Healthcare**
- **Retail**
- **Hospitality**
- **Media and Entertainment**

The questions prompted executives to reflect on security and fraud prevention changes across contact centers and IVR channels over 2022 and their plans for 2023 and beyond. The goal included a better understanding of authentication processes, types of fraud attacks, and what companies are doing to offer personalized, secure services across digital and voice channels. It covered current and planned uses of different technologies, attempting to understand how organizations strive for the optimal balance of usability, efficiency, and security. For the first time, we asked respondents how their contact center security process performed so that we could apply the methodologies described in “Unlock Your Call Centre” ([www.unlockyourcallcentre.com](http://www.unlockyourcallcentre.com)) at an aggregate level to identify opportunities for improvement.



## Conclusions

Progress is always slower than we might like and expect. The clear result of this survey is that although some organizations have started to transition to modern security methods, few are yet to realize their full potential. The only practical way for many organizations to address the tidal wave of increased contact center demands in a commercial way is by increasing automation, and now that the majority are on modern cloud-based platforms, the technical barriers to automation are far smaller than the practical challenge of poor rates of identification and authentication. This survey also shows that for many organizations, one or more modern authentication methods have significant potential to increase automated authentication rates such that the power of modern voice self-service solutions can be realized.

Fortunately, respondents plan to address these challenges, with 92% expecting an increase or significant increase in their authentication and fraud prevention budgets next year, coming on top of 68% who have already seen increases in 2022.

**For more information on becoming an Opus Research client or to purchase the report, please contact:**

**Pete Headrick**  
**Managing Director, Opus Research**  
e | [pheadrick@opusresearch.net](mailto:pheadrick@opusresearch.net)  
p | +1-415-904-7666

## About Opus Research

Opus Research is a diversified advisory and analysis firm providing critical insight on software and services that support multimodal customer care. Opus Research is focused on “Conversational Commerce,” the merging of intelligent assistant technologies, conversational intelligence, intelligent authentication, enterprise collaboration and digital commerce. [www.opusresearch.net](http://www.opusresearch.net)

**For sales inquires please e-mail [info@opusresearch.net](mailto:info@opusresearch.net) or call +1(415) 904-7666**

This report shall be used solely for internal information purposes. Reproduction of this report without prior written permission is forbidden. Access to this report is limited to the license terms agreed to originally and any changes must be agreed upon in writing. The information contained herein has been obtained from sources believe to be reliable. However, Opus Research, Inc. accepts no responsibility whatsoever for the content or legality of the report. Opus Research, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Further, Opus Research, Inc. shall have no liability for errors, omissions or inadequacies in the information contained herein or interpretations thereof. The opinions expressed herein may not necessarily coincide with the opinions and viewpoints of Opus Research, Inc. and are subject to change without notice.

Published April 2023 © Opus Research, Inc. All rights reserved.