



Securing the Contact Center

16 December 2019 By: Krista Tedder

Walk through a contact center and you will hear violations of security and privacy in the name of servicing the consumer. As we collected information on location at multiple contact centers, it was readily apparent that contact center security needs a makeover. Large and small financial institutions, processors, merchants, and technology companies were assessed to determine best-in-class standards of contact center security; however, a best-in-class solution was not found. Every contact center had significant vulnerabilities that were identifiable by speaking with agents and operational staff, and by listening to consumer conversations.

From the information gathered in the art of the conversation to the data validated to verify the caller, all rely on the weakest link of security—humans. With a sophisticated toolkit, criminals can spoof calls, artfully gather data, and take over accounts without the representative being aware that the true person is not on the call. Or worse yet, when account and transaction information is modified for someone perceived to be a close relation (spouse, child, or executive assistant), the account is at risk.

Contact centers are generally not where security professionals reside, yet it is the front door for criminal activity. A maze of outsourced providers—attributable to necessity or design—provides minimal infrastructure for the building of protective barriers in the contact center itself. No one group is given the funding or the staff required to solve the challenges that contact centers bring. The only way to stop the trend of account takeover is through a collaborative approach and by deploying new security technology.

Key questions discussed in this report:

- What types of fraud occur when contact centers are not secure?
- How are contact centers secured when there are multiple entry points?
- What technology capability is needed to minimize the threats faced by financial institutions and merchants?

Javelin conducted tours of contact center facilities, speaking with executives within internal operations, and with business process outsource companies. Calls of conversations were evaluated to determine the ease of using authentication technology and to understand how key performance metrics were evaluated.

Fraud trend analysis in this report is based on a random-sample panel survey of 5,000 U.S. adults, fielded in November 2018.

- For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level.

Organization spend and priority data in this report is based on information collected in a random-sample panel of 800 information technology security decision-makers, 200 of whom work in financial services.

- For questions answered by all 800 survey respondents, the maximum margin of sampling error is ± 3.46 percentage points at the 95% confidence level.
- For questions answered by all 200 financial services respondents, the maximum margin of sampling error is ± 6.93 percentage points at the 95% confidence level.
- The maximum margin of sampling error is higher for questions answered by segments of respondents.

The consumer payments data in this report was primarily collected from the following:

- A random-sample survey of 3,000 respondents conducted online in March 2019. The overall margin of error is +/-2% at the 95% confidence level for questions answered by all respondents.
- A random-sample survey of 3,000 respondents conducted online in October-November 2017. The overall margin of error is +/-1.74% at the 95% confidence level for questions answered by all respondents.
- A random-sample survey of 10,768 consumers in an online survey conducted in July 2017. The margin of sampling error is $\pm 0.94\%$ at the 95% confidence level.

Copyright ©2020 Escalent and/or its affiliates. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent.

javelinstrategy.com

inquiry@javelinstrategy.com

925.225.9100