After SMS One-Time Passwords: Meeting the Authentication Needs of Banks and Their Customers

19 March 2018 By: Al Pascual, Kyle Marchini

SMS one-time passwords (OTPs) have permeated nearly all authentication experiences in financial services, but because of an increasing number of vulnerabilities, their ability to provide robust security against fraud is failing. Fraud has become prevalent. It is time for financial institutions and others who require identity verification to plan for the next generation of authentication. To be effective, an authentication solution must be secure, user-friendly, instantaneous, and cost-effective, taking the context into account in analyzing the cost and inconvenience of the process and the benefit of its use.

This original report, sponsored by Boloro, examines the use and degradation of SMS one-time passwords, along with the qualities that made it so pervasive, and charts a path forward for institutions in search of a viable replacement.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

Download Whitepaper

Please fill out the form below with a valid email address and we will email you a link to the whitepaper.

This research report was sponsored by:

It was independently produced by:

Consumer data was collected from an online survey of 5,000 U.S. adults over age 18; this sample is representative of the U.S. census demographics distribution. Data collection took place from November 1-16, 2017. Final data is weighted using 18+ U.S. Population Benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS census. For questions answered by all 5,000 respondents, the maximum margin of sampling error is ±1.39 percentage points at the 95% confidence level.

Further data was taken from an online survey of 5,028 individuals fielded from November 5-21, 2016. For questions answered by all 5,028 respondents, the maximum margin of sampling error is ±1.40 percentage points at the 95% confidence level.

Data on bank adoption of authentication features was collected by Javelin with a two-stage process. Results from 28 of the largest depository financial institutions were initially collected through a network of mystery shoppers with at least one active account at each financial institution. Once the mystery shopping had been completed, each financial institution was contacted and given the opportunity to validate the results. Twenty-one financial institutions validated the results of the scorecard. Results for financial institutions that declined to validate results were confirmed by Javelin personnel who held at least one account at each financial institution.

Additionally, Javelin conducted interviews of senior financial industry executives responsible for authentication at U.S. retail banks.

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100