FORRESTER®

Improve Your Customer Authentication Strategy With More Secure One-Time Passwords

Organizations Must Be Proactive With OTP Fraud Prevention Techniques

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY NEUSTAR, MARCH 2022

Table Of Contents

Project Team:
Andrew Magarie,
Principal Market Impact Consultant

Ben Anderson,
Associate Market Impact Consultant

Contributing Research:
Forrester's Security & Risk Management research group

ABOUT FORRESTER CONSULTING

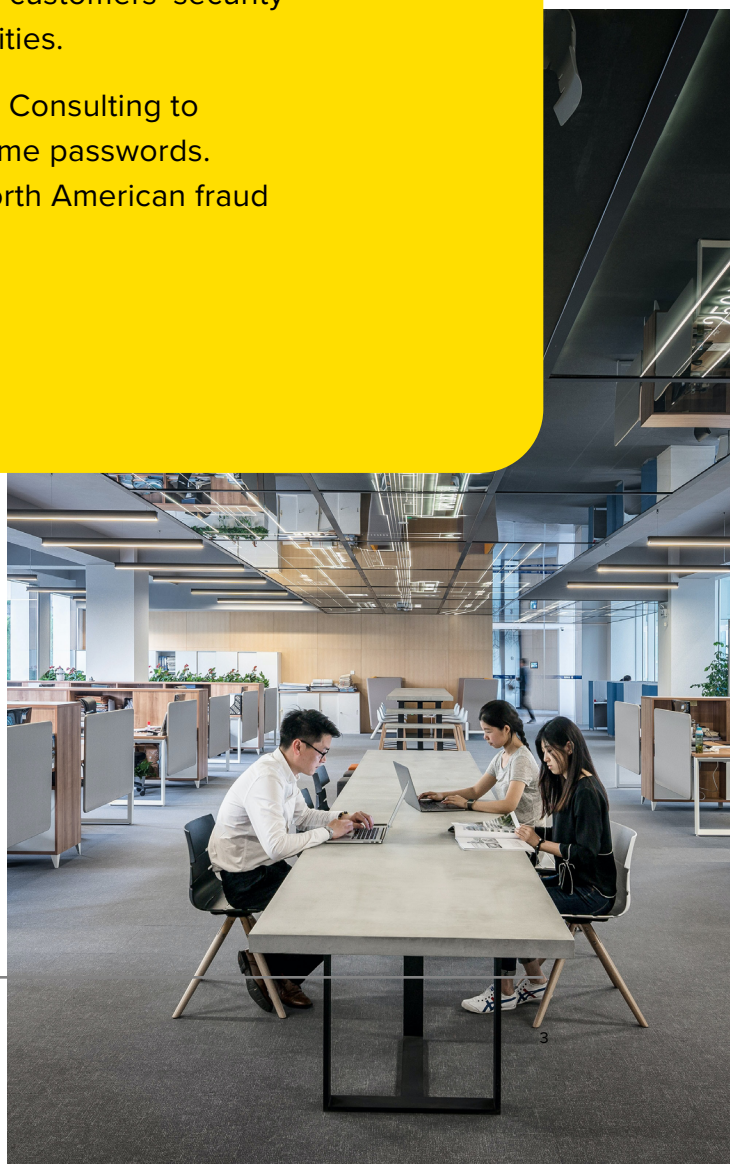
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

In customer authentication, there is a difficult balance that organizations must strike between security and usability — because customers expect both. Most firms use multiple layers of customer authentication to find this balance with each method presenting pros and cons. Ideal methods are accessible to all customers, simple to use, and secure. One-time passwords (OTP) sent directly to a customer's device of choice are perceived to check all three of these boxes with text message OTPs being the most popular option. However, as mobile fraud continues to grow, organizations must improve their text OTP security protocols to maintain safety — or they may lose not only revenue, but customer trust and market share as well.

Many organizations lack the capabilities and technologies needed to effectively prevent and mitigate OTP authentication fraud. However, there are solutions that allow organizations to take a proactive stance against mobile fraud and, in doing so, ensure their customers' security and satisfaction during crucial authentication activities.

In January 2022, Neustar commissioned Forrester Consulting to evaluate customer authentication fraud and one-time passwords. Forrester conducted an online survey with 300 North American fraud prevention decision-makers to explore this topic.



Key Findings

Most organizations use SMS OTP authentication to meet customer needs. Almost 60% of respondents' organizations use OTP customer authentication, and the most popular form of OTP is via SMS/text message. Respondents favor using OTP because it is considered applicable to a large portion of the customer base (73%), easy to use (71%), and secure for customers (72%).

With mobile fraud on the rise, SMS OTP authentication is under fire. Almost all organizations are experiencing phone-related fraud with the number of attacks averaging in the double digits per vector. Respondents using SMS OTP report an average of almost 20 SMS OTP fraud incidents in the last year.

Organizations are challenged to prevent OTP fraud. Almost half of respondents report their organizations lack the technology needed to detect OTP fraud, and 42% say it is hard to know and measure when OTP fraud has occurred. Few are confident that their organizations' current solutions can detect and prevent OTP fraud.

Proactive fraud capabilities can help protect organizations. Respondents are looking for technologies to identify high-risk phone numbers before sending OTPs; detect scams in progress using contextual data before initiating an authentication request; and use decisioning data to predict the best channel for authentication.

Protecting Against Customer Authentication Fraud Is A Balancing Act

Protecting customers from authentication fraud is top of mind for fraud decision-makers, but choosing the correct method to do so is not a one-size-fits-all decision. Customer authentication methods must be secure and not overly disrupt the customer experience or introduce undue friction. Forcing customers to download an application may exclude less tech-savvy populations, while requiring a call to a call center may frustrate an otherwise happy and loyal customer. Further complicating the decision, attitudes towards authentication vary by consumer group. For example, younger smartphone users are more likely to want passwordless authorization than older users.[1] Selecting the right authentication method(s) is critical, as customer authentication fraud impacts customer loyalty, brand reputation, revenue, and more.

Customer authentication fraud erodes customer trust, damaging brand reputation and customer loyalty.

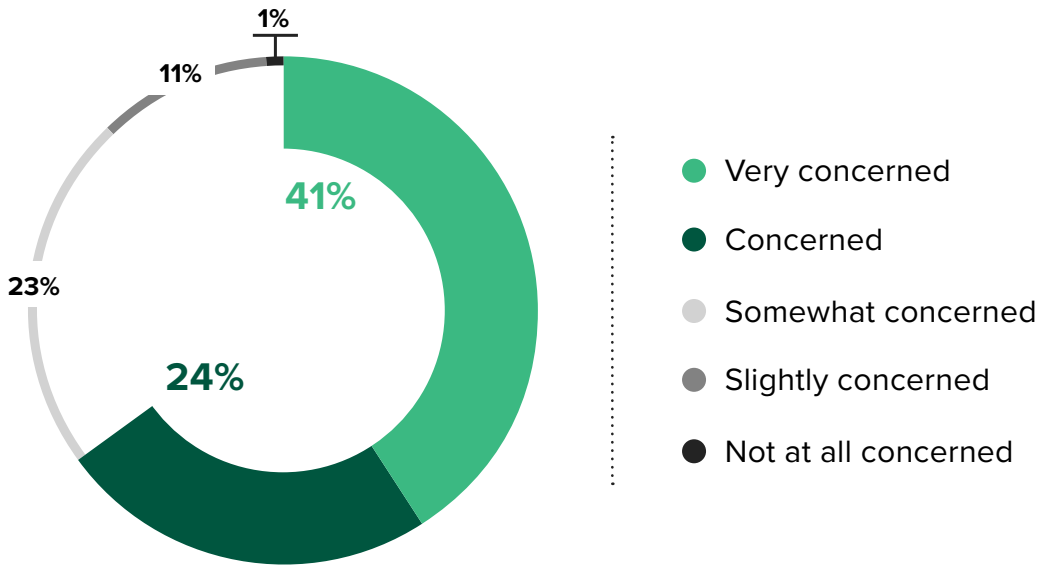
In surveying 300 North American fraud prevention decision-makers, we found that:

- **Customer authentication fraud is a threat to customers and businesses alike.** There are multiple victims in customer authentication fraud and multiple ways that fraud hurts an organization. Customer authentication fraud erodes customer trust, damaging brand reputation and customer loyalty. It costs firms money and market share. With so much on the line, authentication fraud is top of mind for decision-makers. Almost two-thirds of respondents report they are concerned about customer authentication fraud with another 23% somewhat concerned (see Figure 1).
- **Authentication threat is not expected to go away.** With more customer touchpoints and digital interactions on the rise, customer authentication fraud is expected to remain a serious threat. Two-thirds of respondents say that authentication fraud will increase or remain constant over the next two years.

Figure 1

CURRENT STATE OF CUSTOMER AUTHENTICATION FRAUD

"How concerned are you about fraud related to customer authentication at your organization?"



"How do you expect the rate of fraud related to customer authentication to change in the next two years?

Base: 300 North American fraud prevention decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

- **The cost of authentication fraud is high.** While it is difficult to estimate the true cost of authentication fraud since it has such long-reaching consequences to brand reputation, customer loyalty, and market share, nearly half of respondents say their organizations' fraud loss rate over the last year was greater than 5%.

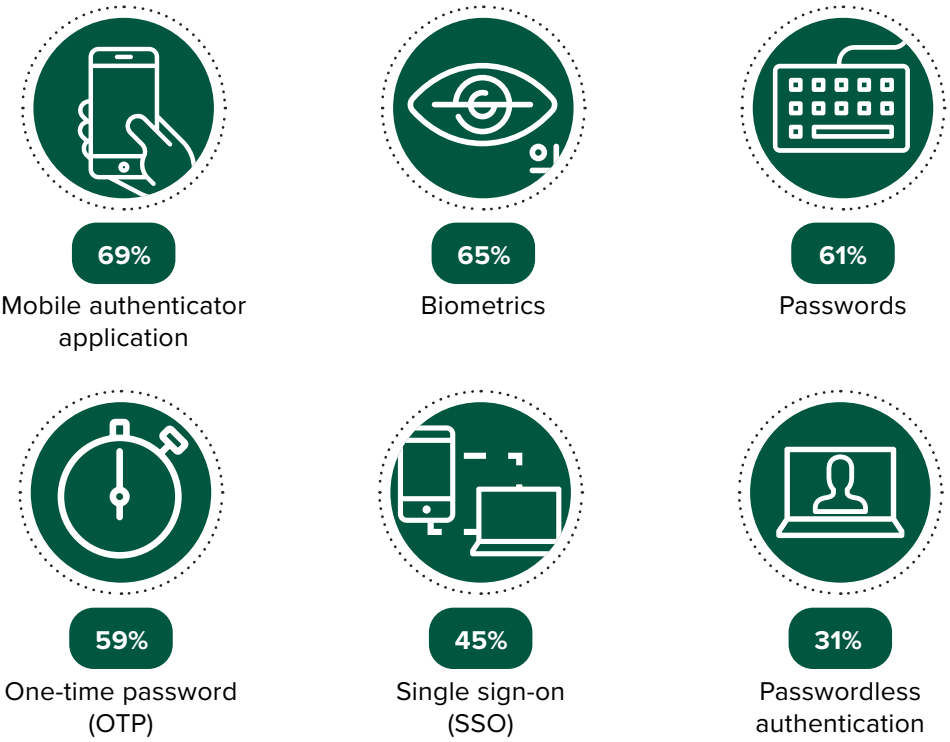
ONE-TIME PASSWORD IS A VERSITILE AUTHENTICATION METHOD

To protect themselves and their customers, most organizations use multiple layers of customer authentication. Nearly eight in ten respondents report their organizations use three or more methods of multifactor authentication (MFA) to prevent fraud (see Figure 2). Each authentication method has varying levels of security, convenience, and complexity, whether it's traditional passwords, different types of biometric authentication (e.g., fingerprints, facial recognition, etc.), or a one-time password sent to a customer through various digital channels.

Mobile authenticator applications are the most prevalent type of authentication respondents' organizations use, but their use requires an application download on a mobile device. This, in turn, requires a smartphone with data usage and the willingness to download a company application. Biometrics are considered secure but require specialized hardware.

Figure 2

"Which of the following methods does your company use for customer authentication?" (Select all that apply.)



Nearly eight out of 10 respondents reported using three or more methods.

Base: 300 North American fraud prevention decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

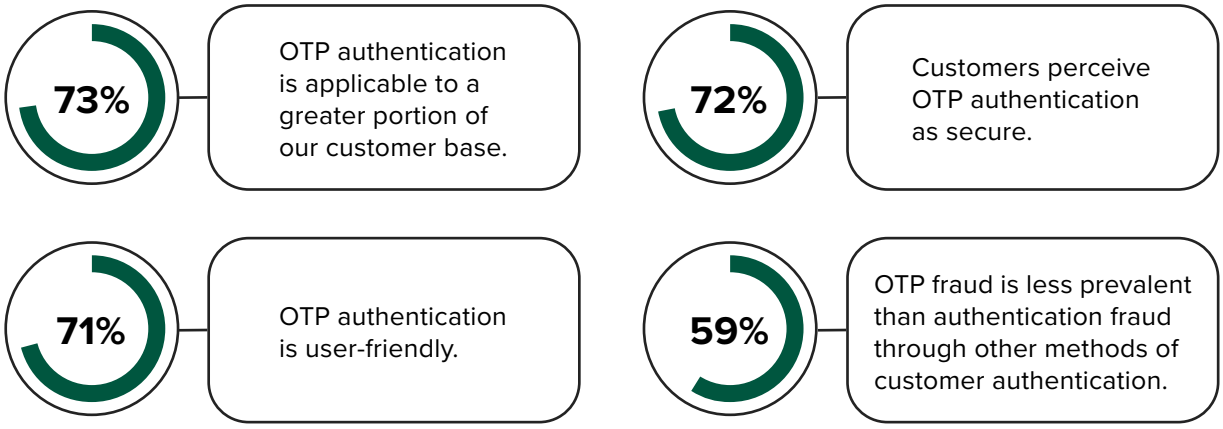
Passwords can be either a security risk or a potential source of user friction, depending on requirement complexity. OTP is perceived as both secure and user-friendly. With this method, a company sends a password to a touchpoint the customer specifies to verify the customer's identity.

The respondents in our survey say:

- **OTP is a popular customer authentication method.** Almost 60% of respondents in our survey use OTP as part of their organizations' customer authentication strategy. On average, those respondents use OTP to protect four interaction points on the customer journey with the most popular being: account login, changes to account information, monetary transactions, and mobile wallet provisioning.
- **OTP is considered both user-friendly and secure.** OTP is a versatile authentication method that can be delivered over a number of ubiquitous communication methods today, including email and text/SMS message. Because of this, OTP is considered by respondents as applicable to a larger portion of the customer base than other methods (73% agree) (see Figure 3). In addition, customer perception of OTP is favorable. Seventy-two percent of respondents say customers perceive OTP authentication as secure, while 71% of respondents say that OTP authentication is user-friendly.

Figure 3

"Why do you use OTP authentication over, or in addition to, other methods of customer authentication?"



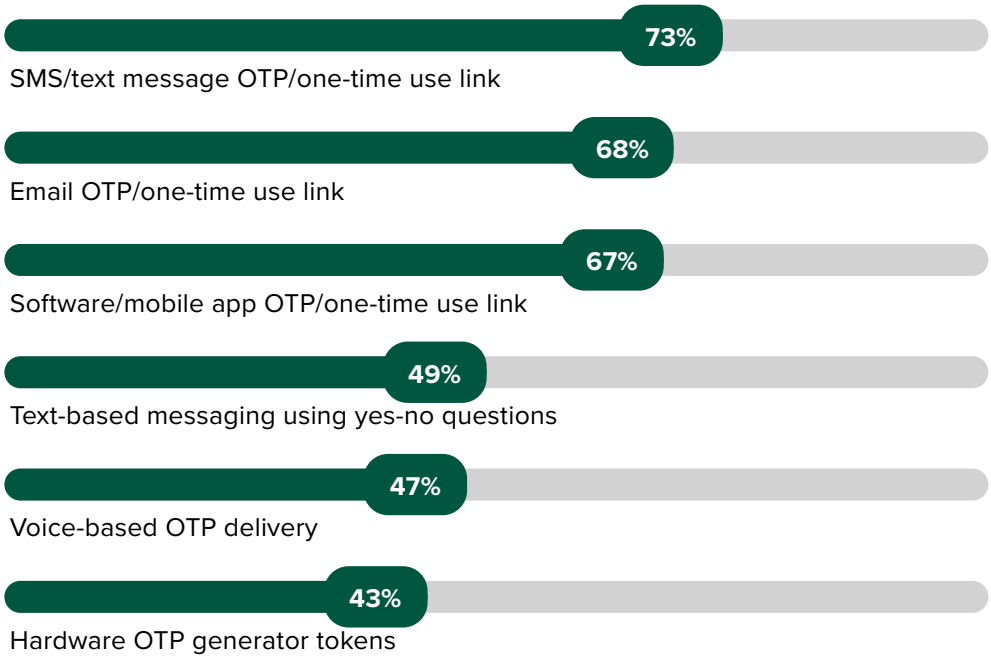
Base: 300 North American fraud prevention decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

- **SMS/text is the most frequently used type of OTP.** Any customer that can send and receive texts can use OTP authentication via text message. This covers more of the population than smartphone users and doesn't require web data to use. Since the text goes directly to a phone, which is presumably in the user's possession, it is considered both safe and easy to use. For these reasons, SMS/text message OTP is the most used OTP method: 73% of surveyed respondents using OTPs do so via SMS/text (see Figure 4). In addition, 83% of respondents who use SMS OTPs say OTPs are the primary method of multifactor authentication their organization uses today. Finally, SMS/text was the most preferred method of OTP delivery among all respondents, even those that do not currently use OTP.

83% of respondents who use SMS OTPs say they are the primary method of multifactor authentication their organizations currently use.

Figure 4

"What types of OTP authentication does your company use?"
(Select all that apply.)



Base: 176 North American fraud prevention decision-makers using OTP authentication
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

Mobile Is A More Vulnerable Channel Than Customers Realize

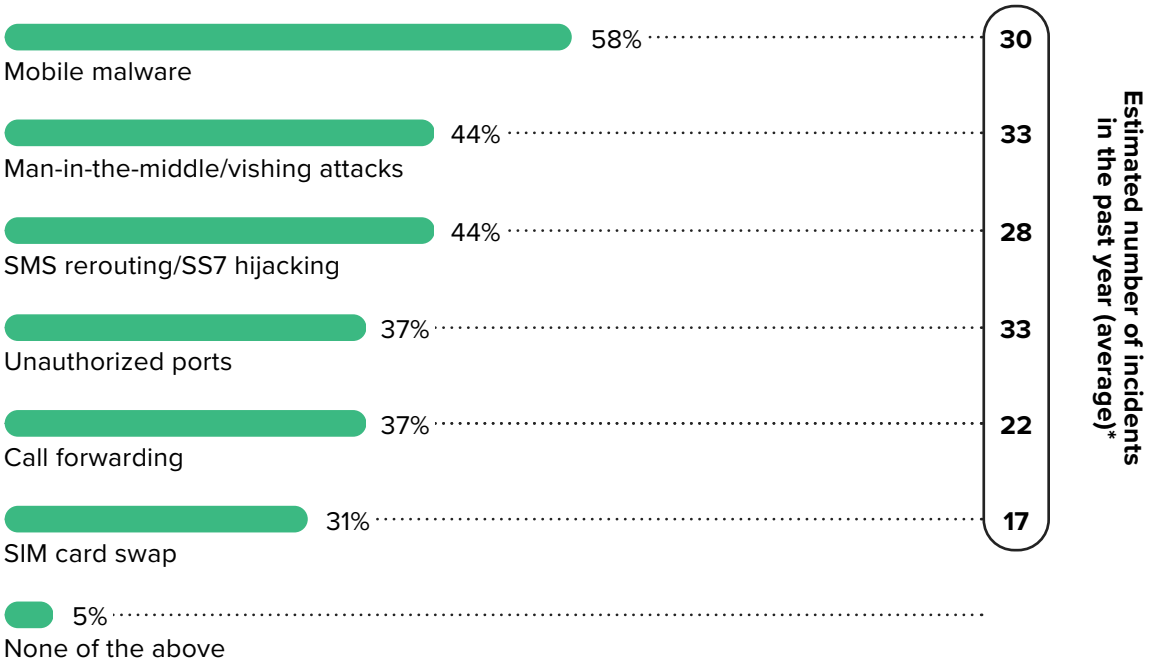
Since mobile phones are always in a user's possession, they are perceived as being secure, especially in the case of a password sent directly to that phone when requested. However, fraudsters have numerous ways to compromise a phone even if it is still in the possession of its owner, and these types of attacks are prevalent today — whether customers know it or not.

- **Phone-related fraud is rife at organizations today.** Almost every respondent in our survey reported that their organizations dealt with some type of mobile fraud in the past year with the number of attacks averaging in the double digits per attack vector (see Figure 5). The most prevalent types of mobile fraud in the last year were mobile malware (58%), man-in-the-middle/vishing (44%), and SMS rerouting/SS7 hijacking (44%).

Figure 5

CURRENT STATE OF MOBILE FRAUD

"What types of fraud techniques has your company experienced in the last year?" (Select all that apply.)



Base: 300 North American fraud prevention decision-makers
*Base: Variable fraud prevention decision-makers that experienced the fraud technique in the past year
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

- **SMS OTP fraud attacks are commonplace.** While 59% of respondents say that OTP fraud is less prevalent than attacks through other customer authentication methods, OTP users still report that their organizations experience dozens of attacks per year, even through mobile. Respondents using SMS OTP reported an average of 34 incidents of OTP fraud in the last year; over half of those incidents related to SMS OTPs.
- **And these numbers may be lower than actual attacks.** One of the main challenges that OTP users report is that their organizations lack the technology to detect OTP fraud (46%) (see Figure 6). And 42% say it is hard to know and measure when OTP fraud has occurred. Given this, OTP fraud incidents may be even more prevalent than reported.

Almost every respondents' organization dealt with some type of mobile fraud in the past year with the number of attacks averaging in the double digits per attack vector.

CURRENT CAPABILITIES FAIL TO MITIGATE FRAUD THREAT

Unfortunately, most survey respondents admit their organizations lack the capabilities needed to effectively prevent and mitigate OTP authentication fraud.

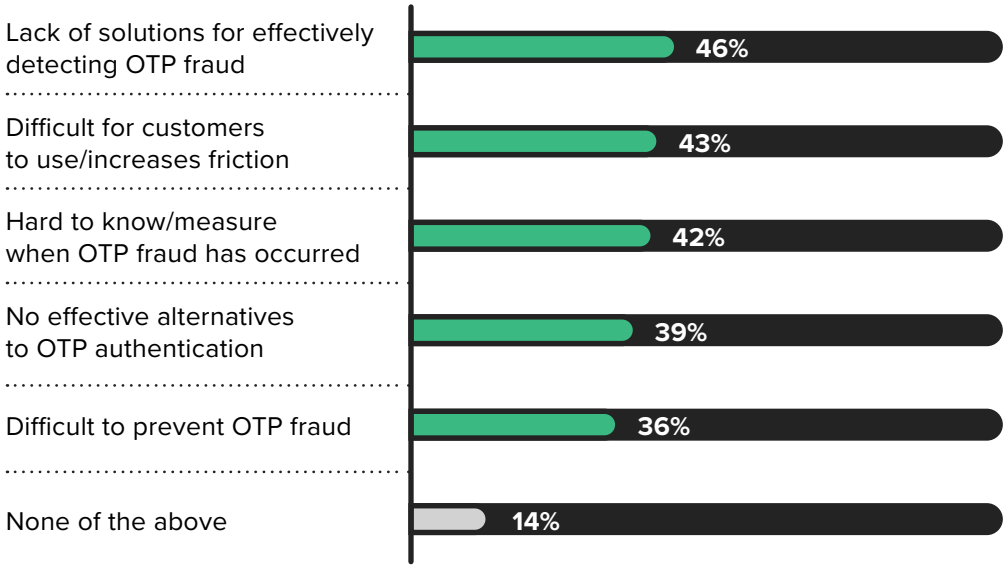
- Only one-in-three respondents say their organizations' ability to prevent OTP fraud is optimized today.
- Few respondents are confident their organizations have the technology needed to solve challenges detecting (30% very confident) and preventing (32% very confident) OTP fraud.

34%

of respondents say their organizations' ability to prevent OTP fraud is optimized today.

Figure 6

“What are your organization’s greatest challenges to using OTP authentication?” (Select all that apply.)



Base: 176 North American fraud prevention decision-makers using OTP authentication
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

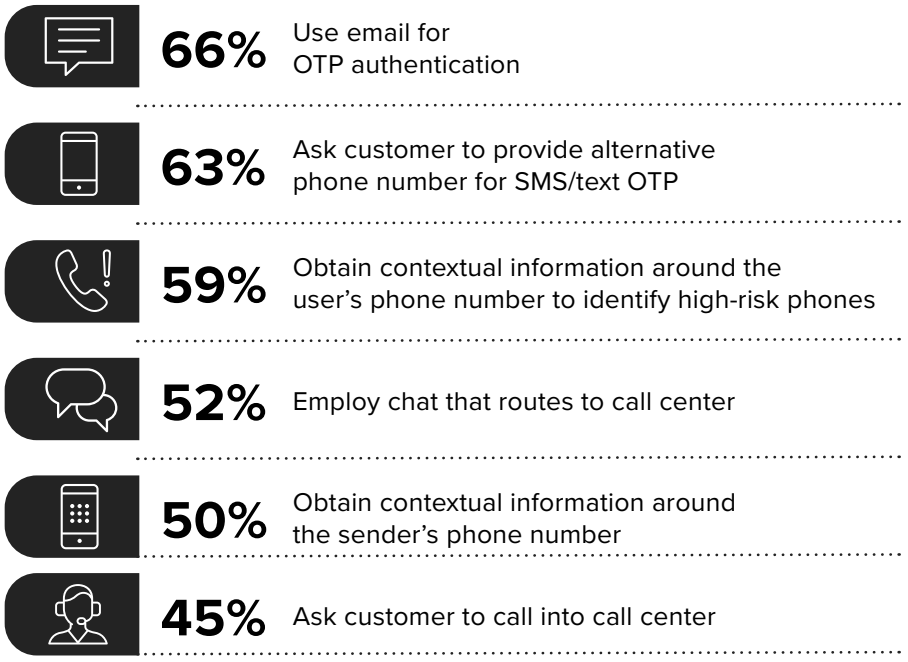
Organizations Must Be Proactive With Their OTP Fraud Prevention

Customer authentication fraud carries heavy costs for organizations and customers alike. Even methods perceived as secure like SMS OTP are targets for malicious fraudsters. To stay ahead of their attackers, fraud decision-makers can choose one of two paths. The first is to look for alternative ways to verify identity, the second is to detect and mitigate risk factors of fraud.

- **Current strategies involve alternative identification.** To stop SMS OTP fraud, organizations are pursuing several alternatives (see Figure 7). Nearly two-thirds of respondents noted their organizations have switched to the less popular email OTP method, and a similar amount have used alternative phone numbers. Both alternatives introduce additional friction to the customer experience, requiring new channels that may not be available or of the customer's preference.

Figure 7

"Which of the following strategies has your company adopted to mitigate SMS/text OTP authentication fraud risk?" (Select all that apply.)



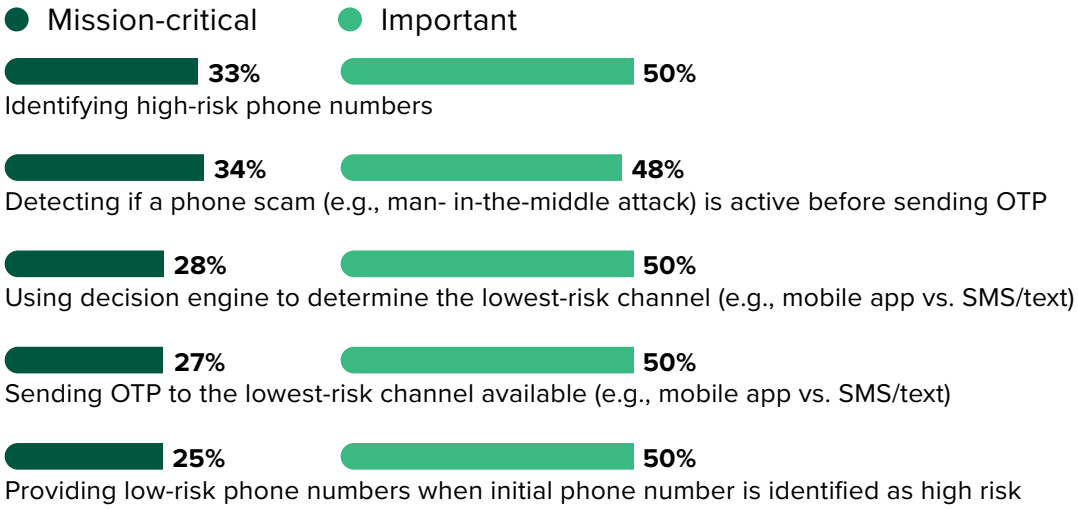
Base: 128 North American fraud prevention decision-makers using SMS OTP authentication
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

Similarly, more than half have directed customers to a chat/call center. Given call centers' reputations as both a security risk, because of lax, inadequate authentication of customers and exposure to social engineering attacks, and as a channel of last resort for customers, it's obvious why this alternative is less than ideal from the security and customer experience perspective.[2] Alternatively, three out of five respondents are trying to proactively mitigate fraud risk by identifying high-risk phone numbers using contextual information about the number.

- **Decision-makers look for capabilities to help prevent OTP fraud.** Rather than introducing potential friction and impacting the customer experience, most decision-makers would prefer to be proactive in detecting OTP fraud and are looking for technology and partners to help them do so. Almost seven in 10 respondents have invested in technology to help prevent OTP incidents. The most important solution capabilities respondents identified to prevent SMS OTP fraud were the ability to identify high-risk phone numbers (83%), the ability to detect a scam in progress before sending the OTP message (82%), and using decisioning to determine the best OTP channel for use (78%) (see Figure 8).

Figure 8

"What future requirements would you consider important in order to prevent the risk of SMS/text OTP fraud?"



Base: 300 North American fraud prevention decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, January 2022

Forrester's in-depth survey of North American fraud prevention decision-makers about customer authentication fraud and one-time passwords yielded several important recommendations:

Use risk-appropriate authentication to keep customer friction low.

Application-based authentication may be one of the most secure methods of customer authentication, but many consumers do not want to download another application and some cannot use them at all. Select MFA methods that best balance risk and ease of use to keep customers safe and satisfied.

Verify all components, including phone numbers, in your MFA strategy.

Fraudsters are searching for the vulnerabilities in your MFA strategy. Often, phone numbers are the weakest link. Verify the phone numbers you are sending authentication requests to. The ability to identify high-risk numbers through contextual data is considered a critical capability for doing so.

Allow customers to select their own MFA methods.

The goal is to serve customers in the context and channel of their choosing. Allowing customers to select their own MFA method provides a convenient, easy authentication experience, minimizing user friction.

Step up authentication to identify problems early.

Analysis of authentication activity can give you insight into unseen weak points and potential threats. Track operational metrics, such as failed registrations and logins, to be proactive with identifying and preventing customer authentication fraud.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 300 decision-makers at organizations in the US and Canada to evaluate customer authentication fraud and one-time password usage. Survey participants included decision-makers in fraud prevention, finance/accounting, IT, and risk and compliance responsible for customer authentication fraud strategy, half of whom work for financial services companies. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study was completed in January 2022.

Appendix B: Demographics

REGION	
United States	**49%**
Canada	**51%**

COMPANY REVENUE	
$500M to $999M	**45%**
$1B to $4.99B	**29%**
$5B to $9.99B	**12%**
$10B or more	**14%**

TOP 4 INDUSTRIES	
Financial services	**50%**
Consumer services	**9%**
CPG/CPM	**8%**
Retail	**6%**

DEPARTMENT	
Fraud prevention	**32%**
Finance/accounting	**27%**
IT/IT security	**27%**
Risk and compliance	**9%**

RESPONDENT TITLE	
C-level executive	**30%**
Vice president	**27%**
Director	**43%**

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

“The Current State Of Enterprise Passwordless Adoption,” Forrester Research, Inc., January 19, 2022.
“An Effective Customer Authentication Strategy Requires Customer Segmentation,” Forrester Research, Inc., January 27, 2021.
“Best Practices: Customer Call Center Authentication,” Forrester Research, Inc., March 22, 2019.

Appendix D: Endnotes

[1] Source: “An Effective Customer Authentication Strategy Requires Customer Segmentation,” Forrester Research, Inc., January 27, 2021.
[2] Source: “Best Practices: Customer Call Center Authentication,” Forrester Research, Inc., March 22, 2019.


FORRESTER®