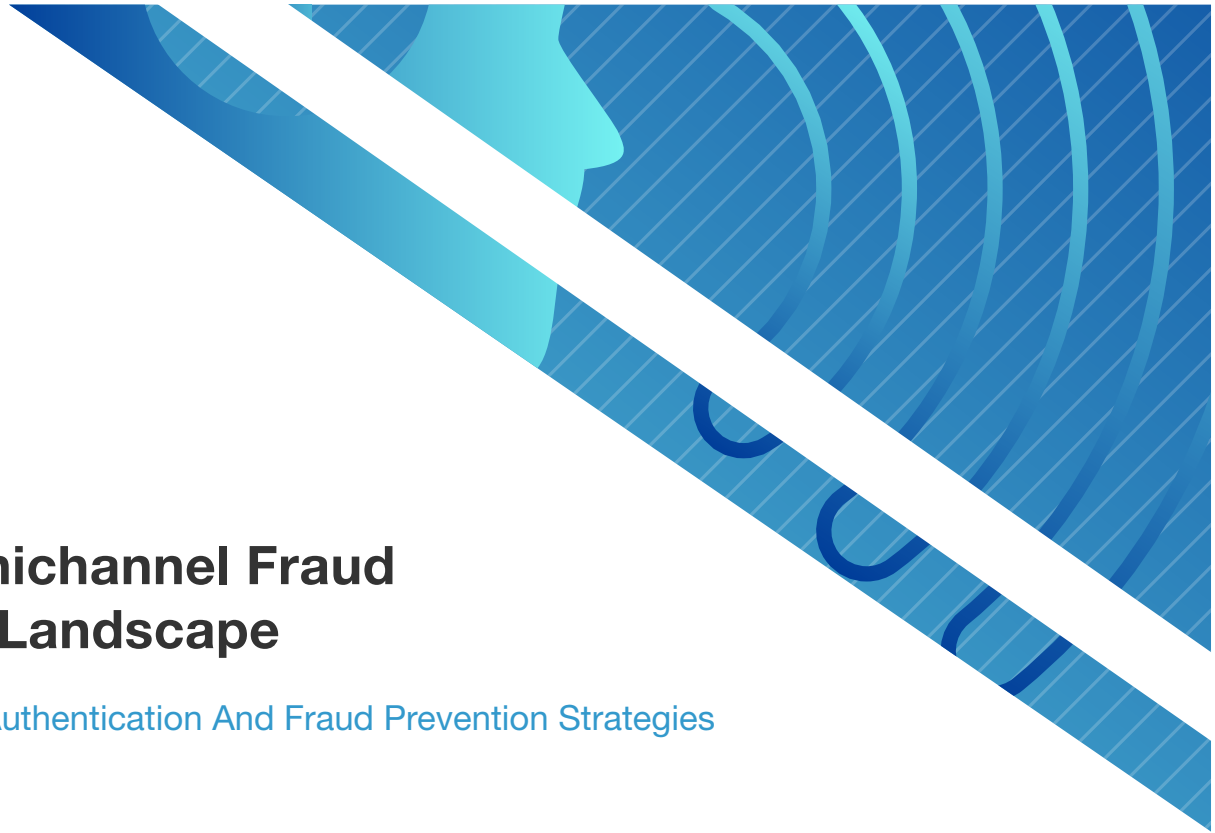
FORRESTER®



Navigating The Omnichannel Fraud And Authentication Landscape

How Biometrics Power Modern Authentication And Fraud Prevention Strategies

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY NUANCE | JUNE 2019

The Authentication And Fraud Prevention Paradigm Is Shifting

Brands have traditionally focused on voice in the contact center to authenticate customers and prevent fraud. However, as customer expectations for speedy, seamless interactions increase, self-service digital channels like mobile applications and chat are exploding — and with it, the risk of fraud. As firms work to meet expectations for swift and frictionless digital experiences, they're finding the need to shift their authentication strategies to suit working across channels to protect customers and the business.

In April 2019, Nuance commissioned Forrester Consulting to evaluate fraud and authentication. With our survey of 561 fraud and authentication decision makers across the globe, we sought to understand which channels are targeted, how organizations are responding, and how brands can improve.

Key Findings

Cross-channel fraud is the new normal. Just as customers access services across channels, fraudsters work cross-channel to exploit vulnerabilities. Cross-channel authentication is critical.

Firms are underprepared to combat cross-channel fraud. Despite confidence in fraud prevention in individual channels, firms are far less confident in their cross-channel prevention capabilities.

Biometric authentication methods are key to a modern cross-channel strategy. Firms using biometrics in more than one channel are more likely to describe their cross-channel fraud prevention as fully or nearly optimized.

As Digital Authentication Skyrockets, New Fraud Risks Emerge

Mobile and digital experiences are in high demand — and the growth of authentication on those channels is substantial: 67% of companies have seen a 10% or greater increase in authentication on their mobile applications in 24 months. And as companies change how they connect with customers, they are shifting how they view and manage fraud risk:

- 70% agree that traditionally voice channels have been the focus of fraud prevention strategy.
- 74% agree that opening up new channels for customer engagement has increased their vulnerability to fraud.
- 87% agree that they're now focused on fraud prevention in digital channels.

Rank of channels where firms experience the highest levels of customer authentication	Percent of firms that have seen customer authentication increase 10% or more over the past 24 months on this channel
Website	55% →
Mobile application	67% →
In-person	25% →
Phone	28% →
Chat	54% →

Base: Variable executives with responsibility for fraud prevention and customer authentication at companies globally
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

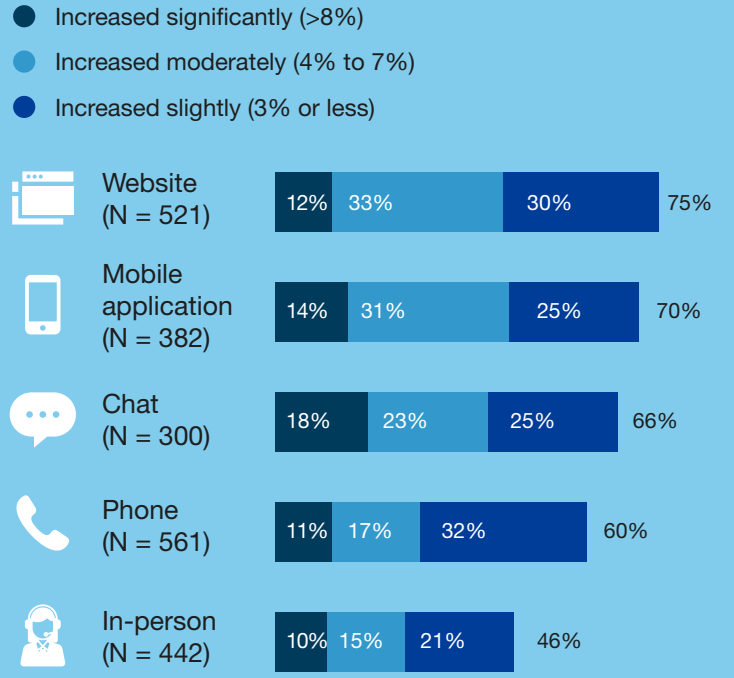
Fraud Is On The Rise — And No Channel Is Safe

Unfortunately, rapid adoption on the part of customers for on-demand, digital services has led to comparable increases in the rate of fraud in digital channels: 45% of firms experienced a 4% or greater increase in the rate of fraud on their mobile applications and websites in the past 24 months.

Meanwhile, despite the success of "mobile-first" strategies to empower digitally savvy customers, phone and in-person channels are also growing in terms of both authentication and fraud at many firms. Although 87% of firms say they're focused on fraud prevention in digital channels, companies' legacy channels clearly still need protection.

Digital channels are the greatest target of fraud, but legacy channels can't become a blind spot.

"How has the rate of fraud (including fraud detected before it happened and discovered after it occurred) changed over the past 24 months for the following channels?"



Base: Variable executives with responsibility for fraud prevention and customer authentication at companies globally
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

Firms Are Overconfident In Their Ability To Prevent Fraud In Individual Channels

Despite growing fraud, firms believe their prevention ability is mature: Up to 84% say their ability to prevent fraud on any one channel is nearly or fully optimized.[1] However, firms are overconfident — they rely on many of the same easily defrauded authentication methods:[2]

- **Personally identifiable information (PII):** confirmation of birth dates, ZIP codes, etc.; data that is often available via social media or purchased on the dark web following a breach.
- **Knowledge-based authentication (KBA):** i.e., "what was the color of your first car?"; decreasingly secure data due to high-profile breaches or is so obscure that it frustrates users.
- **Passwords:** often not complex enough or users write them down in insecure places; fraudsters will try leaked password combinations across many sites in the hopes the same password has been reused.

"For each of the channels listed, select the ways your company enrolls, authenticates, and/or authorizes customers for that channel."

Top five authentication methods - riskiest methods are in white

PHONE

Identity verification
Personally identifiable information
Knowledge-based authentication
Risk-based authentication
Passwords

WEBSITE

Passwords
Identity verification
Personally identifiable information
Knowledge-based authentication
Software-based OTP

MOBILE APP

Passwords
Identity verification
Personally identifiable information
Knowledge-based authentication
Software-based OTP

IN-PERSON

Identity verification
Personally identifiable information
Knowledge-based authentication
Fingerprint biometrics
Face biometrics

Base: Variable executives with responsibility for fraud prevention and customer authentication at companies globally
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

Cross-Channel Fraud Is The Greater Threat

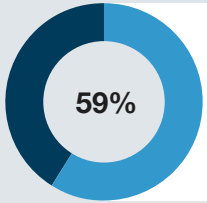
While most firms feel they have individual channels under control, fraudsters are at work across channels, exploiting the vulnerabilities of each. For example, card-not-present (e.g., using a stolen credit card number without a physical card) is an old fraud tactic but remains effective on the phone channel, while account takeover (e.g., password hacking) is effective on websites and mobile apps.

As a result, 82% of firms agree that authentication across channels is increasingly critical to fraud prevention. Yet only 59% define their cross-channel fraud prevention as nearly or fully optimized — far less mature than any one channel. Firms are underprepared to combat the changing nature of fraud.

"What type of fraud has been most common on each channel over the past 24 months?"

Channel	Most common type of fraud
Mobile application and website	Account takeover
Phone	Card-not-present
Chat	ID theft
In-person	Synthetic ID fraud

Only 59% describe their firm's ability to prevent fraud across channels as nearly or fully optimized.



Well below the average maturity of any one channel (81.2%)

Base: 561 executives with responsibility for fraud prevention and customer authentication at companies globally
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

Preventing Cross-Channel Fraud Improves Customer Experience

As firms work toward cross-channel fraud prevention, they view improved customer experience (CX) as a key outcome. Unsurprisingly, it outranks any cost reduction benefit, likely due to CX's well-established link to revenue growth.[3] Improved CX comes from cross-channel authentication experiences that are:

- **Effective:** limiting false rejects and false accepts, even as customers move across channels.
- **Easy:** authentication methods that are not frustrating or burdensome and that are kept consistent across channels.
- **Emotionally resonant:** customers feel good about their experience — for example, trust is an especially important emotion to connect to authentication.[4]

"What business benefits are to be gained by better preventing cross-channel fraud?"

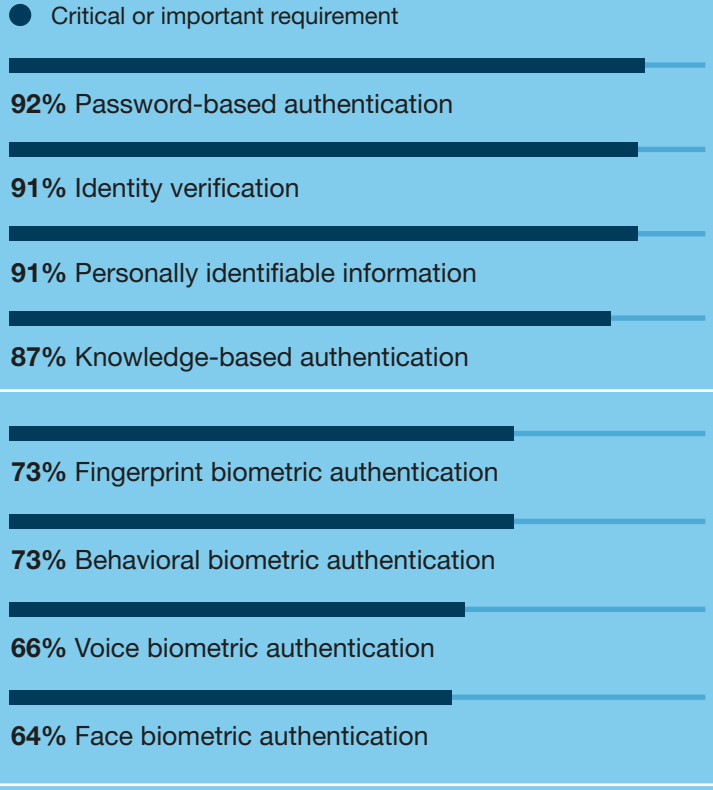
Base: 561 executives with responsibility for fraud prevention and customer authentication at companies globally
*Note: Net Promoter and NPS are registered service marks, and Net Promoter Score is a service mark, of Bain & Company, Inc., Satmetrix Systems, Inc., and Fred Reichheld.
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

Biometrics Help Firms Balance Security And Customer Experience

To improve cross-channel authentication, prevent fraud, and benefit from better CX, firms are evaluating legacy and emerging authentication methods. Despite clear drawbacks, firms still feel passwords, PII, and KBA prevent fraud. However, they also see value in biometrics. Based on innate characteristics, these methods do not add friction to the interaction.[5] In addition, biometrics can identify imposters regardless of the knowledge or social engineering skills they have. Firms using biometrics cross-channel are:

- Less likely to rely on passwords and PII on mobile application, website, and phone (by as much as 24 points).
- More likely to describe their fraud prevention in each channel as optimized (by as much as 20 points).
- More likely to describe their cross-channel fraud prevention as fully or nearly optimized (by 9 points).

Firms still feel that aging forms of authentication are important, but many see the value in biometrics



Base: 561 executives with responsibility for fraud prevention and customer authentication at companies globally
Source: A commissioned study conducted by Forrester Consulting on behalf of Nuance, April 2019

Conclusion

Companies are in a perpetual race to provide services when, where, and how their customers prefer. This has led to a necessary shift in the way firms think about authentication and fraud prevention. Both legitimate customers and fraudsters move freely across channels — firms need a modern authentication toolset that can balance the needs of security with the demands of CX. Emerging tools like biometrics are gaining importance, not only for their relative security compared with outdated methods, but for their ability to smooth and enhance customer experience. Firms using biometrics in more than one channel are beginning to move the needle on cross-channel fraud prevention.

Project Director:
Emma Van Pelt,
Market Impact Consultant

Contributing Research:
Forrester's security and risk research group

Methodology

This Opportunity Snapshot was commissioned by Nuance. To create this profile, Forrester Consulting leveraged existing research from Forrester's security and risk research group. We supplemented this research with custom survey questions asked of 561 global fraud and authentication decision makers. The custom survey began and was completed in April 2019.

ENDNOTES

RETURN 1. An optimized fraud prevention program is defined as one that is continuous and effective, integrated, proactive, and usually automated.
RETURN 2. Source: "Top Cybersecurity Threats In 2018," Forrester Research, Inc., November 27, 2017.
RETURN 3. Source: "The US Customer Experience Index, 2018," Forrester Research, Inc., June 19, 2018.
RETURN 4. Source: "Drive Growth With Customer Trust And Build Brand Resilience," Forrester Research, Inc., September 25, 2018.
RETURN 5. Source: "Best Practices: Behavioral Biometrics," Forrester Research, Inc., May 5, 2018.

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.

Demographics

REGIONS

- Europe: 55%
- The Americas: 36%
- Australia: 9%

POSITION

- C-level: 39%
- VP: 24%
- Director: 37%

NUMBER OF EMPLOYEES

- 500 to 999: 1%
- 1,000 to 4,999: 54%
- 5,000 to 19,999: 29%
- 20,000 or more: 16%

INDUSTRY

A range of industries is represented, including financial services, retail, telecommunications, manufacturing, technology, professional services, shipping, and healthcare.

FORRESTER®