What's next

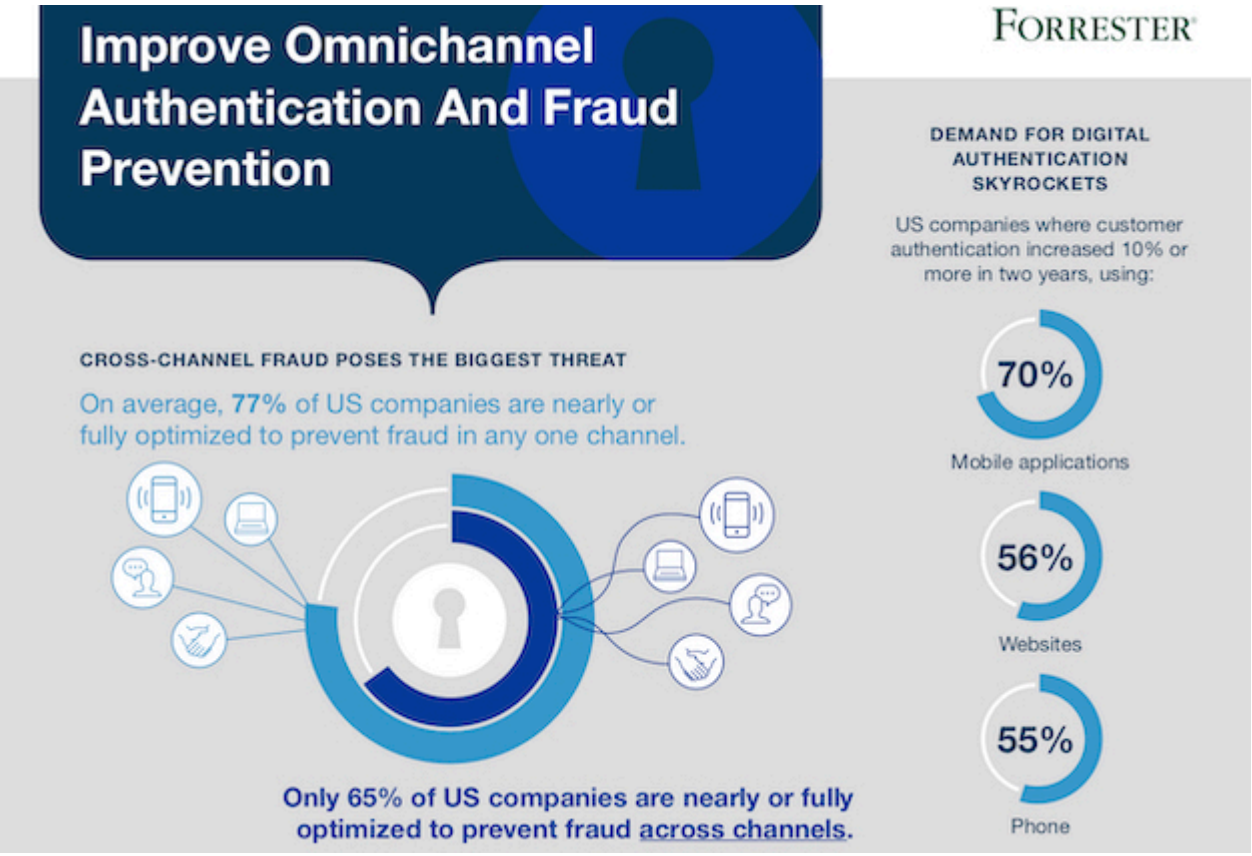
Enterprise

Authentication and fraud prevention requirements in the omni-channel world

Authentication and fraud prevention used to be a problem exclusively for the contact center when fraudsters would call with stolen or synthetic credentials. That's changed with consumers' insatiable appetites for low effort, self-service digital channels coupled with fast, frictionless experiences. Nuance commissioned Forrester to understand which channels fraudsters are targeting, how organizations are responding, and how brands can improve.

Jon Bornstein

Posted September 30, 2019



When financial institutions, telcos, governments and other organizations talk about authenticating customers and preventing fraud, the conversation has historically centered on the contact center. This was especially true in the age of call centers when the primary way that consumers engaged was by picking up the phone and talking with live customer service agents.

While voice is still an important way that brands engage with customers (especially for escalations), it now complements lower effort, self-service digital offerings that consumers increasingly prefer. The proliferation of chat, mobile apps, web and other digital interaction channels requires brands to broaden their authentication and fraud prevention strategies to cover the omni-channel and its varied components.

The sea change in channels and consumer expectations is happening at breakneck speed. To help contact center, risk, and security clients keep pace, Nuance commissioned Forrester to deconstruct the evolving omni-channel authentication and fraud prevention landscape.

Forrester surveyed more than 500 North American executives and found that:

- Customer authentication in mobile and web channels is exploding. Not surprisingly, fraudsters are watching this behavior because fraud in digital channels now outpaces telephone fraud.
- In response, organizations are shifting their fraud prevention strategies from voice to

digital channels, as well as implementing cross-channel authentication

- The biggest challenge to success is that many firms rely on PINs, passwords, and knowledge-based authentication questions – data that's cheap and readily available on the dark web
- In response, biometrics is a strategy many are looking to, including voice, behavioral, facial and fingerprint
- This is because firms using biometrics in more than one channel report that they're better able to keep up with fraudsters

The takeaway is that security and CX can co-exist. Learn more in the Forrester study and its companion on-demand webinar with Andras Cser, VP and principal analyst – both available here (registration required).

Tags: authentication, Call Center Fraud, contact center, fraud, Omnichannel Customer Service, security, Voice Biometrics

More Information

Understanding the landscape
Equip yourself with this Forrester Consulting Opportunity Snapshot and its companion webinar, infographic, and 36 second video.
Learn more

About Jon Bornstein

Jon leads North America marketing programs for Nuance's Security & Biometrics business unit. He partners with industry experts to communicate the value of the company's biometrics solutions in improving customer authentication and reducing fraud. His career spans multinational marketing roles at companies such as Deltek, SAS Institute and Porter Novelli.

View all posts by Jon Bornstein