The new biometrics mandate in financial services.

Authentication and fraud prevention across voice and digital channels.

NUANCE®

Table of contents

1 The PIN and password era is over / p2

2 The new mandate for better authentication and fraud prevention: biometrics across multiple channels / p3

3 Layered defenses = more choices, better security / p4

4 What customers want: better security and a better experience / p5

5 Case study: Royal Bank of Scotland Group / p6

6 Case study: Virginia Credit Union / p8

7 The next wave in security: Nuance Biometrics / p9

The PIN and password era is over

Countless reasons why PINs and passwords just don't work anymore

Too many passwords

A Nuance survey found that consumers manage an average of 11 online accounts and must remember nine different passwords to access those accounts.

Too easily forgotten

And users forget them. Nuance found that 28% of consumers call a contact center every three months to reset login credentials – and 10% are doing this more than once a week, creating too much friction, too much effort, and too much expense to make them feasible for authentication.

Too many incidents

The frustrating reality is that PINs and passwords just don't deter fraud any longer. Nearly one-fourth of consumers worldwide have been victims of fraud within the past year – with an average cost of $2,000. U.S. citizens were hardest hit: 38% in the same period.[1]

Too easy to crack

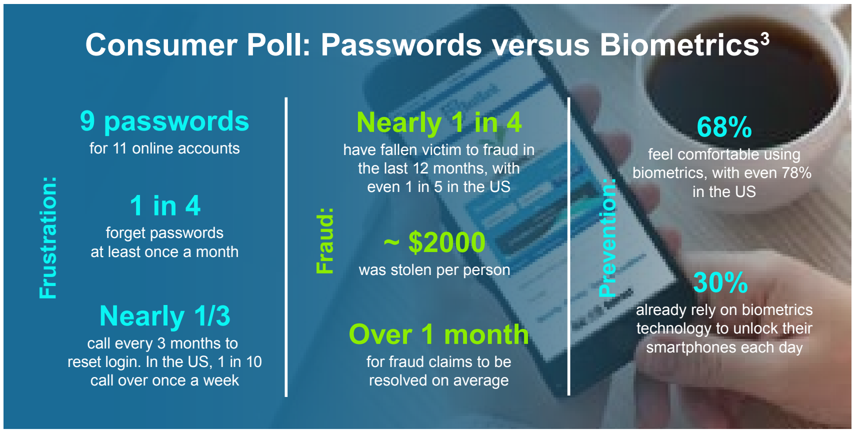
As Forrester notes, an eight-character, non-dictionary password with two nonidentical numbers, one uppercase letter and two special characters can be cracked… in just nine hours. As exponentially greater computing capacity becomes commonplace, it's clear that the password will no longer be up to the task of protecting payments and other high-risk transactions.[2]

Too many password breaches

Consumers and institutions alike know the truth: An unending stream of data breaches and compromises of personal data and user credentials has taken its toll. In just the past year, we've seen Facebook expose 540 million user accounts. Hackers took 106 million accounts from CapitalOne. Similar breaches have taken place at Equifax (145 million accounts), Heartland Payment Systems (130 million accounts), Target (110 million accounts), Epsilon (250 million accounts) and Experian (15 million accounts) – all leaving consumers vulnerable.

Too many attacks causing too much damage

While the losses can reach billions of dollars, fraud wipes out more than accounts. It wipes out customer trust, corporate reputation and public confidence – sometimes permanently.



Consumer Poll: Passwords versus Biometrics[3]

Frustration:

9 passwords
for 11 online accounts

1 in 4
forget passwords at least once a month

Nearly 1/3
call every 3 months to reset login. In the US, 1 in 10 call over once a week

Fraud:

Nearly 1 in 4
have fallen victim to fraud in the last 12 months, with even 1 in 5 in the US

~ $2000
was stolen per person

Over 1 month
for fraud claims to be resolved on average

Prevention:

68%
feel comfortable using biometrics, with even 78% in the US

30%
already rely on biometrics technology to unlock their smartphones each day

2019

A busy year for fraud

540M accounts exposed at Facebook

250M accounts exposed at Epsilon

145M accounts exposed at Equifax

130M accounts exposed at Heartland Payment Systems

110M accounts exposed at Target

106M accounts exposed at CapitalOne

15M accounts exposed at Experian

[1] https://whatsnext.nuance.com/customer-experience/world-password-day-fraud-prevention/

[2] Forrester Research TechRadar: Biometric Authentication, Q1 2017 "Adoption of User- and Mobile-Friendly Biometrics will Kill the Password." Andras Csar and Alexander Spiliotes, March 14, 2017.

[3] Survey methodology: Nuance Communications commissioned OnePoll to conduct an online survey of 1,000 adults (18+) in each of UK, US, Australia, Germany and Spain (5,000 participants in total). The survey was carried out between 9th – 18th April 2019.

The numbers are staggering

A 2018 study by Javelin Strategy & Research reports that identity-fraud victims increased 8 percent to 16.7 million U.S. consumers vs. the previous year. Fraudsters netted 1.3 million more victims in 2017, stealing $16.8 billion from U.S. consumers. Account takeovers (ATOs) tripled over the past year, resulting in $5.1 billion in losses. Victims paid an average of $290 out of pocket and wasted 15 hours each to resolve these incidents.[4]

Customers are demanding a better way: World-class banks, brokerages, insurers, and other financial services firms are under tremendous competitive pressure to provide faster, friendlier access to customers while strengthening security to prevent fraud.

"As users increasingly demand frictionless authentication everywhere, biometrics solutions have garnered significant attention for both authentication and fraud prevention especially… Furthermore, as their adoption increases, they will hasten the demise of the industry's least user-friendly method — passwords."

Forrester Research, "TechRadar™: Biometric Authentication, Q1 2017

The new mandate for better authentication and fraud prevention: biometrics across multiple channels

According to Aite Group, less than half (42%) of executives at financial institutions (FIs) believe their current authentication processes are effective.[5] Thanks to a range of data breaches fraudsters seemingly have all the data they need to defeat KBA questions and launch phishing attacks, malware, and social engineering tactics in contact centers. And outdated authentication vulnerabilities are now overmatched.

For a growing number of FIs, a comprehensive, omni-channel fraud-prevention strategy starts with biometric authentication. With biometrics, FIs first recognize and verify a person's identity through a unique physical or behavioral trait – like the way a person talks. Voice biometrics is a popular option for authenticating customers in interactive voice response systems and with live contact center agents. Behavioral biometrics is especially valuable in chat, mobile, web and other digital applications. These and other techniques can be used – passively and actively – to confirm a customer's identity.

Beyond authentication, biometrics can detect fraud in those same voice and digital channels. The reason is that fraudsters follow customers: If they identify a weak link in the FIs' defenses, they'll attack them.

Forward-thinking FIs recognize that securing the omni-channel requires a mix of biometric technologies. They're increasingly using a combination of modalities to achieve strong gains in efficiency and security while giving customers' choice for low-effort, frictionless experiences. The strength of biometrics becomes significantly greater when different techniques are used in combination to prevent fraud.

1/4

of consumers worldwide have been victims of fraud within the past year – with an average cost of $2,000 each.

[4] Pascual, Al; Marchini, Kyle; and Miller, Sara. (February 6, 2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Javelin Strategy & Research. Retrieved from: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#

[5] "The Biometrics Win-Win: Reduce Fraud and OpEx While Improving CX" – Aite Group – July 2019

Cross-channel fraud: A closer look[6]

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 individuals, firms are far less confident in their cross-channel prevention capabilities.

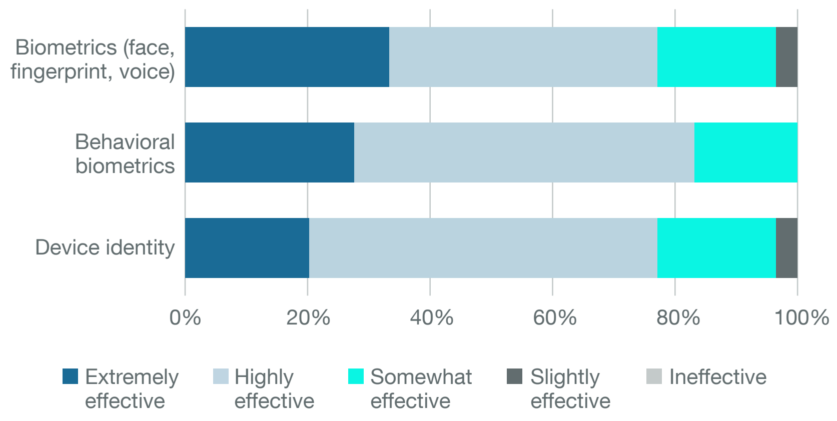
Biometric authentication methods are key to a modern cross-channel strategy. Firms using biometrics in more than one channel are more likely to describe their cross-channel fraud prevention as fully or nearly optimized.

Layered defenses = more choices, better security

While there are many different styles of biometric fraud prevention, the real power emerges when they're combined into a multi-modal protocol. Most experts believe that it's unlikely that one specific modality will emerge as a dominant choice for financial institutions. More likely, companies will need to employ strategies that layer together multiple biometric modalities.

A multi-modal approach is smart for many reasons and a strategy that many financial services providers are already pursuing. From a customer-experience standpoint, it's important that FIs respect clients' choice in how they want to engage. Whether that's by calling, chatting, messaging or any new communications channel, each method requires that the client be authenticated. Biometrics is unique in its ability to do that across channels seamlessly.

Q. Please rate the effectiveness of the following for mitigating financial crime. (n=29 to 30)



Source: Aite Group survey of 32 financial fraud professionals, September 2018

Forrester notes cross-channel fraud is the greater threat[6]

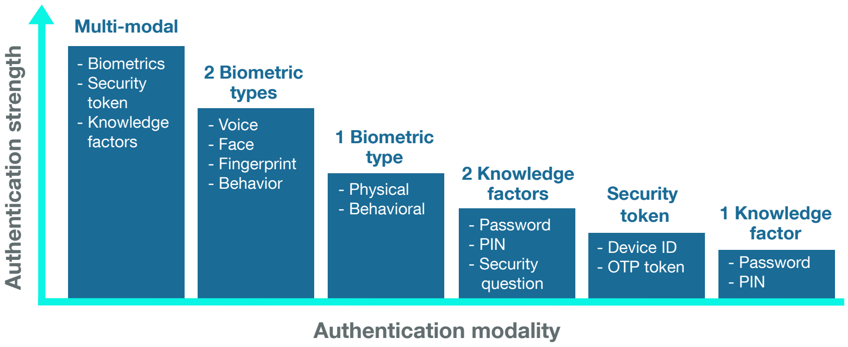
"While most firms feel they have individual channels under control, fraudsters are at work across channels, exploiting the vulnerabilities of each. For example, card-not-present (e.g., using a stolen credit card number without a physical card) is an old fraud tactic but remains effective on the phone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

$30B

ABI Research projects that the global biometrics market will exceed $30 billion by 2021, with banking and personal finance companies leading the charge.

[6] "Forrester Opportunity Snapshot: Navigating The Omni-channel Fraud and Authentication Landscape" – A custom study commissioned by Nuance - June 2019.

Secondly, a multi-modal approach represents a powerful step up for security workflows. For example, a quick fingerprint scan in a mobile banking app might enable a customer to access the account balance or perform low-level account management functions — but a request to transfer money, pay bills, or apply for a line of credit might trigger a request for voice authentication.



What customers want: better security and a better experience

Each individual technology represents a significant improvement in customer experience over PIN- and password-based authentication — and most provide substantial gains in efficiency and security as well. They authenticate seamlessly and offer strong security advantages that PINs and passwords cannot.

Importantly, from a privacy standpoint, biometric data is not stored in an identifiable way on either mobile devices or in the backend databases that provide authentication. Even if a hacker obtains the device or penetrates the database, the information (typically a cryptographic key) is impossible to reassemble in a usable fashion.

Secondly, biometric data is extremely hard to fake. The most sophisticated technologies in use today include "liveness detection" features that determine the difference between an actual person and pre-recorded or synthesized voice. This is especially important for FIs: Aite Group estimates that losses from synthetic identity fraud will almost double from 2015 to 2020.[7] Organizations need to be assured their fraud prevention solution providers have the resources and expertise to stay ahead of this growing problem.

Another important consideration is the efforts that FIs can make to prevent fraud before it occurs. FIs needn't confine themselves to a defensive posture, continually thwarting attacks from a typically small number of fraudsters. Instead, biometrics can help them mount counteroffensives to identify perpetrators who often respond by shifting their attacks to different FIs. Biometrics also help FIs gather more evidence to help prosecute criminals. Since these crime rings often use their ill-gotten proceeds to finance human trafficking or terrorism, there's a heightened sense of urgency to root them out and prevent their operations.

↑ **Better CX**
Operational efficiencies

"A strong business case can be made for a robust biometric solution that provides value across the enterprise, improves the CX, and results in strong operational efficiency improvements."

– Aite Group.[8]

400^{M}

Nuance security and biometrics technology is used by more than 400 million consumers to make more than 8 billion successful and secure transactions every year. Nuance omni-channel customer engagement technology is being implemented by 19 of the 20 world's largest financial institutions today.

$2^{B}

Between 2018 and 2019, Nuance Security & Biometrics solutions helped clients prevent more than $2 billion in fraud losses.

[7] Conroy, Julie; Aite Group; "Synthetic Identity Fraud: The Elephant in the Room"; May 3, 2018; https://www.aitegroup.com/report/synthetic-identity-fraud-elephant-room

[8] "The Biometrics Win-Win: Reduce Fraud and OpEx While Improving CX" – Aite Group – July 2019

Case study: Royal Bank of Scotland Group

Like any bank, the call center is an important customer service channel for the Royal Bank of Scotland Group (RBS), which serves 19 million customers across 12 banking and financial services brands.

But the voice channel is also a prime target for fraudulent activity. To combat criminal behavior—both from lone-wolf attackers and organized crime networks—RBS was looking for ways to get a clearer view of fraud indicators across all its customer engagement channels.

The bank needed to put more effective security mechanisms in place while still delivering a fast, smooth experience for genuine customers. That meant finding ways to rely less on passwords and other static identifiers that can be stolen or forgotten, and it knew that voice biometrics could be an important piece of the anti-fraud puzzle.

RBS deployed Nuance Security & Biometrics to screen every incoming call and compare voice characteristics (including pitch, cadence, and accent) to a digital library of voices associated with fraud against the bank. The software quickly flags suspicious calls and alerts the call center agent to potential fraud attempts.

Challenge

- Serve 19 million customers across 12 banking and financial services brands
- Identify fraud indicators (from lone-wolf attackers and organized-crime networks – across all customer-engagement channels, particularly voice)
- Move from passwords to voice biometrics for faster customer interactions while ensuring strong security

Solution

- Nuance Security & Biometrics compares each incoming call to a library of known fraudsters and alerts the call-center agent to potential fraud.
- A whitelist of genuine customers rapidly authenticates genuine customers without passwords or other ID information.
- Nuance ties in other criminal detection tools to detect fraud on digital channels.

Results

- 17 million inbound calls screened, and 23,000 fraud attempts detected.
- One in every 3,500 calls is a fraud attempt.
- One fraudster connected to 1,500 suspicious bank accounts.
- +300% ROI.

RBS
The Royal Bank of Scotland

+300%

ROI reported by RBS.

17M

inbound calls screened.

23K

fraud attempts detected.

As well as a library of ‘bad’ voices, RBS now has a whitelist of genuine customer voices that can be used for rapid authentication, without the need for customers to remember passwords and other identifying information.

The Nuance solution also enables the bank to take a holistic approach to fraud detection and prevention. By combining Nuance data with information from other criminal activity detection tools, RBS has discovered that fraudsters on the voice channel also perpetrate a lot of fraud on digital channels. Armed with that knowledge, the bank has been able to identify and disrupt organized crime activities to protect its customers and assist law enforcement.

In less than a year, RBS has screened 17 million inbound calls. Of these, 23,000 have led to alerts, and the bank has found that one in every 3,500 calls is a fraud attempt. Stopping fraudsters in their tracks is already paying off financially, as Jason Costain, the bank’s head of fraud strategy and relationship management, explains: “Although this initiative isn’t just aimed at reducing losses, we expected to save a reasonable amount of money, and we’ve already saved one and a half times that. The ROI [from Nuance] is probably well over 300%, so as payback from a technology deployment, it’s been very impressive.

“It’s not just about stopping financial loss—it’s about disrupting criminals,” says Jason. “For example, one prolific fraudster identified through Nuance was connected to suspect logins on 1,500 bank accounts. That’s helped us protect potential fraud victims and identify the ‘mules’ being used by the crime network to perpetrate fraud, leading to two arrests so far.”

“It’s not just about stopping financial loss—it’s about disrupting criminals.”

Jason Costain, RBS, Head of Fraud Strategy and Relationship Management

Case study: Virginia Credit Union

Virginia Credit Union (VACU), a $3.4 billion institution, fields 3,000 calls per day, so agent-driven authentication required too much time. Biometric technology was appealing because members wouldn't need to do or remember anything, and voice biometrics are considered more secure than outdated PINs, passwords, and knowledge-based questions.

VACU uses Nuance Security & Biometrics to transparently verify a caller's identity by analyzing and comparing more than 100 unique characteristics while the member speaks to the agent. Nuance's advanced voice biometrics help VACU detect known criminals, uncover new fraud patterns, and prevent account takeovers.

VACU agents spend less time authenticating members and more time addressing members' specific needs. Voice ID reduces call-handling times, significantly improves member and agent satisfaction, and maintains a high-touch, high-quality caller experience for members.

Since launch, the VACU Voice ID solution had decreased handle time by 37 seconds/call. With approximately 60,000 agent-handled calls per month, this represents a savings of two FTE per month – and member feedback has been very positive.

Challenge
– Slow, complex, inefficient authentication processes
– Poor caller experience and use of member dollars
– Increasing sophistication of fraudsters

Solution
– Nuance Security & Biometrics quickly ID callers and deters fraudsters
– Connects VACU's existing telephony and backend systems to Nuance APIs
– Custom, desktop pop-up window gives agents seamless, in-call verification

Results
– Overall average handle times decreased by 37 seconds
– Savings equivalent to two full time employees/month
– 79,000+ verified matches in first year
– Design-to-deployment in less than six months

VIRGINIA Credit Union

↓37

Decreased average handle time by 37 seconds per call.

6

months from design to deployment.

79K+

verified matches in the first year.

The next wave in security: Nuance Biometrics

From any perspective and by virtually all measures, the PIN/password model for authentication has passed the end of its useful life. Too many data breaches and other vulnerabilities have left financial institutions unable to deter criminals and prevent fraud without adding unwelcome friction to the customer experience and unnecessary costs to the FI. That’s why more FIs are embracing biometrics across voice and digital channels. With biometrics, companies can transparently, efficiently, and accurately authenticate customers to prevent fraudulent activity and protect customer accounts and assets.

To learn more, visit nuance.com/fraud or email us at CXexperts@nuance.com.

About Nuance Communications, Inc.
Nuance Enterprise is reinventing the relationship between enterprises and consumers through customer engagement solutions powered by artificial intelligence. We aim to be the market leading provider of intelligent self- and assisted-service solutions delivered to large enterprises around the world. These solutions are differentiated by speech, voice biometrics, virtual assistant, web chat and cognitive technologies; enabling cross-channel customer service for IVR, mobile and web, Inbound and Outbound; and magnified by the design and development skill of a global professional services team. We serve Fortune 2500 companies across the globe with a mix of direct and channel partner selling models.

NUANCE®

NUAN–CS–3950–01–WP, Nov 26 2019