

Contact Center AI, Kundeninteraktion auf allen Kanälen

Conversational Banking und Betrugsprävention – wo steht die Finanzbranche?

[Nuance Communications](#)

23 September 2022



Digitale Customer Journeys fordern Banken und Finanzinstitute. Der Bankingclub Germany hat im Auftrag von Nuance Communications nachgefragt: Wie sicher sind Kundendaten? Wo wird in zeitgemäße Biometrie investiert? Welche Bereiche haben am meisten Potenzial?

The security of customer data is a top priority for banks and financial institutions. At the same time, more and more customers want a seamless customer experience across multiple channels – via mobile apps, online, and over the phone. With conversational AI and biometric authentication procedures, the balancing act between customer satisfaction on all channels and the highest level of security is achieved. However, not everyone has reached this point yet.

Wie die Studie vom Bankingclub Germany mit 119 Branchenexperten zeigt, gibt es dabei große Unterschiede: Während im Mobile Banking bereits häufig partielle Biometrie genutzt wird, hat der telefonische Kanal am meisten Nachholbedarf. Dass sich eine solche Investition wirtschaftlich lohnt, zeigt das Beispiel der britischen NatWest Group eindrucksvoll auf: Im ersten Jahr nach der Einführung einer sprachbiometrischen Authentifizierungsmethode konnte ein ROI von 300 Prozent erzielt werden.

Vom Kanaldenken zum Conversational Banking

Das Nutzungsverhalten ist im Wandel: Immer mehr Finanzdienstleistungen werden über digitale Kanäle bezogen. Die Finanzinstitute sind gefordert, eine Customer Experience zu bieten, die digitalen Kanäle wie Messaging und Chat, aber auch Sprachkanäle einbezieht. Herausforderung dabei: Kundenfreundlichkeit und höchste Sicherheit unter ein Dach zu bringen.

The implementation of biometric authentication procedures differs greatly between the different channels. For mobile banking, financial institutions are making use of the biometric authentication methods already available in mobile devices, such as fingerprint or facial recognition. For example, 50 percent of those surveyed say they use biometrics in mobile banking. However, caution is advised here: device-based authentication solutions are more vulnerable and therefore carry greater risks of data theft, fraud and abuse.

Anders sieht es beim Telefonkontakt aus, hier geben nur 19 Prozent an, über biometrische Authentifizierungsverfahren zu verfügen. Obwohl komplizierte Authentifizierung per Passwort oder Abfragen von persönlichen Informationen weder kundenfreundlich noch sicher sind, werden diese nach wie vor von der großen Mehrheit der Bankinstitute eingesetzt. Hier zeigt sich ein wesentliches Potenzial: Biometrische Authentifizierung per Stimme oder Verhalten erhöht nicht nur die Zugangssicherheit signifikant, sondern senkt die Kontaktdauer und fördert die Kundenzufriedenheit. Mit 56 Prozent wird der telefonische Kanal auch in der Selbsteinschätzung als mögliche Schwachstelle bewertet, die behoben werden sollte.

The time of passwords and knowledge-based authentication is over. Not everyone agrees on how to achieve the next level of security. When asked, 67 percent said they actively focus on fraud prevention – leaving a third who take action afterwards in the hope that the damage will be limited. Rather, the banks agree that they are stronger together to take action against fraudsters. In so-called fraud pools, exchanges take place regularly to avoid repetitions of attack scenarios.

In conclusion, the industry experts assessed their institutions as progressive throughout, but the survey also shows where potential lies dormant. In particular, it is worth taking a look at the individual communication channels: Several good authentication methods together are better than any single good authentication method. A less than optimal authentication via fingerprint or face scanner is already many times more secure in combination with voice biometrics. Those who use the very secure methods for voice, behavior and conversation verification in parallel give criminals no chance.

- Stimmbiometrie erstellt einen einzigartigen Abdruck der Stimme und kann innerhalb weniger Sekunden legitime Kunden oder Betrüger erkennen.
- Verhaltensbiometrie erkennt die Personen an der Art und Weise, wie sie tippen, über ihr Smartphone wischen, eine Maus bedienen und andere Faktoren ihres digitalen Verhaltens.
- Gesprächsbiometrie authentifiziert die Kunden anhand der Art und Weise, wie sie Sätze konstruieren, die gewählten Wörter und sogar die Emojis, die sie verwenden.

Conversational Banking: Sicher und kundenzentriert

On the one hand, we understand conversational banking or conversational AI to mean AI-supported authentication in the interaction of voice biometrics, behavioral biometric systems and conversational biometrics for the best possible protection against unauthorized access. But Conversational AI is much more than that: It connects the communication channels and turns a voice dialog system into an intelligent self-service channel with the following advantages for banks and their customers:

1. Individualisiertes Finanzmanagement: immer und überall, Zugriff via Apps.
2. Personalisierte Angebote: proaktive Entscheidungshilfen, Cross-Selling und Upselling.
3. Customer Service: Bequemer Service, nahtlos über mehrere Kommunikationskanäle.
4. Anlageberatung: Der Trend zu KI in der Anlageberatung setzt sich fort.
5. Betrugsprävention: Kontinuierliche biometrische Authentifizierung garantiert Sicherheit.

Längst ist das Kundenerlebnis zu einem der wichtigsten Erfolgsfaktoren für Finanzdienstleister geworden. Die Verwendung von KI in der Customer Journey führt direkt zu besseren Ergebnissen – noch ist Conversational AI ein Wettbewerbsvorteil, bald wird es der neue Standard sein.

In eine sichere Zukunft investieren

Investments are typically measured by ROI. Apart from the fact that avoiding fraud or reputational damage is very difficult to quantify, the investment in fraud prevention is seen as positive throughout. Those who invest in conversational banking gain more than just averting criminal attacks. Conversational banking is an investment in sustainable customer satisfaction, efficient processing times and a step towards a secure future.

Tags: [Betrugsprävention](#)