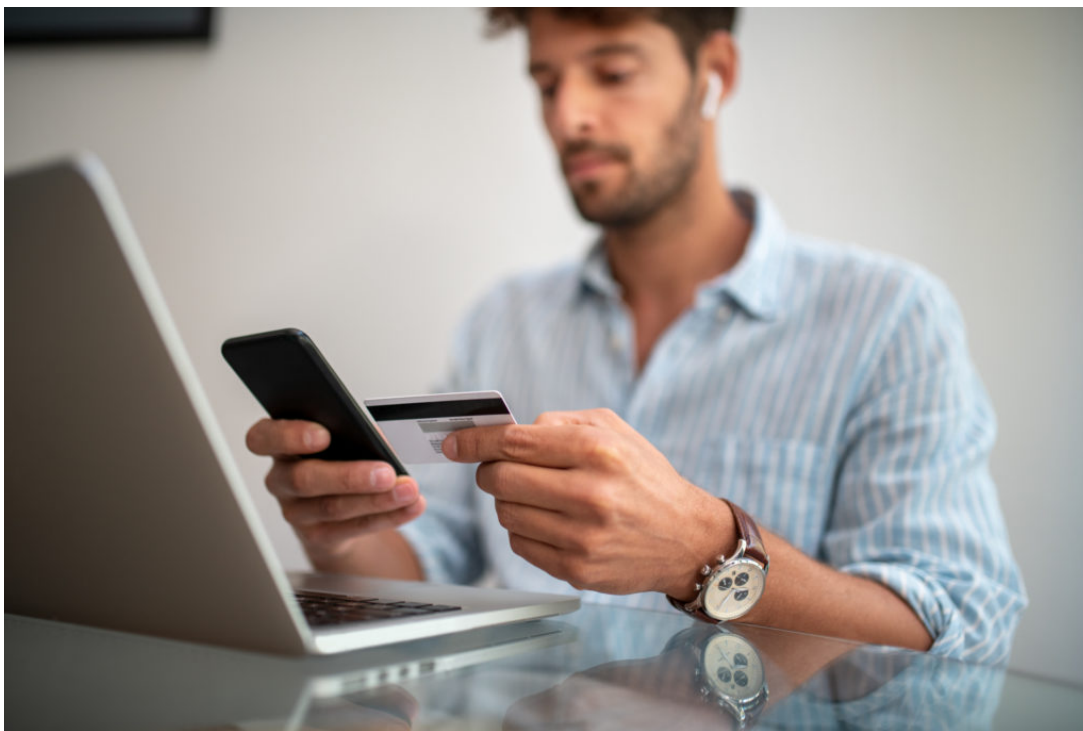


Contact Center AI, Kundeninteraktion auf allen Kanälen

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?

Die Sicherheit der Kundendaten hat bei Banken und Finanzinstituten höchste Priorität. Gleichzeitig wünschen sich immer mehr Kunden eine nahtlose Customer Experience über verschiedene Kanäle - per Mobile-Apps, online und telefonisch. Mit Conversational AI und biometrischen Authentifizierungsverfahren gelingt der Spagat zwischen [Kundenzufriedenheit auf allen Kanälen](#) und einem Höchstmaß an Sicherheit. Noch sind aber nicht alle an diesem Punkt angelangt.

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.

Die Implementierung von [biometrischen Authentifizierungsverfahren](#) unterscheidet sich stark zwischen den verschiedenen Kanälen. Für das Mobile Banking machen sich Finanzinstitute die bereits in den Mobilgeräten vorhandenen biometrischen Authentifizierungsverfahren zu Nutze, wie Fingerabdruck oder Gesichtserkennung. So geben 50 Prozent der Befragten an, Biometrie im Mobile Banking zu verwenden. Doch ist hier Vorsicht geboten: Gerätebasierte Authentifizierungslösungen sind anfälliger und bergen deshalb größere Risiken für Datendiebstahl, Betrug und Missbrauch.

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.

Die Zeit der [Passwörter und wissensbasierter Authentifizierung](#) ist abgelaufen. Wie die nächste Sicherheitsstufe zu erreichen ist, sind sich nicht alle einig. Auf Nachfrage gaben 67 Prozent an, aktiv auf Betrugsprävention zu setzen – damit bleibt noch ein Drittel, die im Nachhinein tätig werden, mit der Hoffnung, dass sich der Schaden in Grenzen hält. Eher einig sind sich die Banken, dass sie gemeinsam stärker sind, um gegen Betrüger vorzugehen. In sogenannten Fraudpools findet regelmäßig Austausch statt, um Wiederholungen von Angriffsszenarien zu vermeiden.

Abschließend beurteilten die Branchenexperten ihre Institutionen durchwegs fortschrittlich, doch zeigt die Umfrage auch auf, wo Potenziale schlummern. Insbesondere lohnt sich ein Blick über die einzelnen Kommunikationskanäle: Besser als jede einzelne gute Authentifizierungsmethode sind mehrere gute Authentifizierungsmethoden zusammen. Eine nicht ganz optimale Authentifizierung per Fingerabdruck oder Gesichtsscanner ist [in Kombination mit Stimmbiometrie](#) schon um ein Vielfaches sicherer. Wer die sehr sicheren Methoden zur Stimm-, Verhaltens- und Gesprächsverifizierung parallel einsetzt, lässt Kriminellen keine 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

Als Conversational Banking oder [Conversational AI](#) verstehen wir einerseits die KI-gestützte Authentifizierung im Zusammenspiel von Stimmbiometrie, verhaltensbiometrischen Systemen und Gesprächsbiometrie für den bestmöglichen Schutz vor unerlaubten Zugriffen. Die Conversational AI ist aber viel mehr als das: Sie verbindet die Kommunikationskanäle und macht aus einem Sprachdialogsystem einen intelligenten Selfservice-Kanal mit folgenden Vorteilen für Banken und ihre Kunden:

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

Investitionen werden typischerweise am ROI gemessen. Abgesehen von der Tatsache, dass die Vermeidung von Betrug oder einem Reputationsschaden sehr schwierig in Zahlen zu fassen ist, wird die Investition in

Betrugsprävention durchwegs positiv gewertet. Wer in Conversational Banking investiert, gewinnt mehr als nur die Abwendung von kriminellen Angriffen. [Conversational Banking ist eine Investition in nachhaltige Kundenzufriedenheit](#), effiziente Bearbeitungszeiten und ein Schritt in Richtung sicherer Zukunft.

Tags: [Betrugsprävention](#)

More Information

Risiken mindern und Kundenzufriedenheit verbessern

Lesen Sie die Studie vom Bankingclub.

[Learn more](#)