Die Bedeutung von Biometrie für PSD2.

Verbessern Sie die Sicherheit elektronischer Zahlungen durch biometrische Authentifizierung.

NUANCE

Finanzdienstleister müssen gewährleisten, dass Transaktionen mit einem Höchstmaß an Sicherheit durchgeführt werden können und dabei einen reibungslosen Kundenservice gewährleisten. Um hier Unternehmen bei der Einhaltung der neuen gesetzlichen Bestimmungen für den Zahlungsverkehr in der Europäischen Union zu unterstützen, bietet Nuance branchenführende biometrische Lösungen.

Zahlungsdiensterichtlinie 2 (PSD2)

Die zweite Zahlungsdiensterichtlinie (Payment Service Directive 2, **PSD2**)[1] ist Teil globaler Bestrebungen im Rahmen der Bankenregulierung, bei denen Sicherheit, Innovation und Wettbewerb im Vordergrund stehen. Die PSD2 trat am 13. Januar 2018 in Kraft, mit einer verlängerten Übergangszeit bis zum 31. Dezember 2020. Die Verlängerung wurde von der Europäischen Bankenaufsichtsbehörde EBA genehmigt, um allen betroffenen Unternehmen die fristgerechte Einhaltung der Vorschriften zu erleichtern. PSD2 zielt darauf ab, die europäischen Zahlungsdienste in der EU zum Nutzen von Verbrauchern und Unternehmen zu modernisieren. Auf diese Weise soll sie es Unternehmen ermöglichen, mit dem sich rasch entwickelnden Markt Schritt zu halten, während gleichzeitig der Verbraucherschutz bei Betrug und Haftung sowie die Rechenschaftspflicht im gesamten Zahlungsverkehr verbessert wird.

Valdis Dombrovskis[2] betont: *„Diese Richtlinie ist ein weiterer Schritt in Richtung des digitalen EU-Binnenmarktes. Sie wird die Entwicklung innovativer Online- und Mobilzahlungen fördern, die der Wirtschaft und dem Wachstum zugutekommen werden.“*

Die neue europäische Richtlinie will nicht nur den technologischen Wandel widerspiegeln, sondern gleichzeitig digitale Innovationen fördern, z. B. durch Erleichterungen bei Einführung neuer Zahlungsdienstleistungen. Darüber hinaus sollen eine größere Gebührentransparenz gewährleistet sowie Verbraucherschutz und Zahlungssicherheit verbessert werden.

PSD2: Wichtigste Änderungen

- Schafft gleiche Wettbewerbsbedingungen für Zahlungsdienstleister, indem es Unternehmen ermöglicht, mit neuen Angeboten in den Zahlungsverkehr einzusteigen.
- Bietet mehr Möglichkeiten im Zusammenhang mit Transaktionen in neuen Regionen und in Fremdwährungen (außerhalb des Euroraums und der EU-Mitgliedstaaten).
- Reguliert neue Zahlungsdienste zwischen Bankkonten (neben Kreditkarten und Überweisungen), z.B. zu Zahlungsaufträgen und Kontoinformationen.
- Erhöht die Sicherheitsanforderungen, inklusive einer starken Kundenauthentifizierung (Strong Customer Authentication, SCA) sowie neuer Verbraucherschutzmaßnahmen.
- Führt Kontrollen im Zusammenhang mit Fällen von Zahlungsbetrug und der Haftung von Zahlungsdienstanbietern ein: Wird ein unautorisierter Zahlungsvorgang durchgeführt, so ist der Finanzdienstleister des Käufers verpflichtet, den Betrag des unautorisierten Zahlungsvorgangs unverzüglich zu erstatten.

1. Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt.
2. Vizepräsident, zuständig für Finanzstabilität, Finanzdienstleistungen und Kapitalmarktunion

Was macht PSD2 so besonders?

Offenes Bankwesen

PSD2 ist ein wichtiger Katalysator, damit „Open Banking“ endlich Wirklichkeit wird. Neue Marktteilnehmer und ihre Dienste für Zahlungsaufträge und Kontoinformation werden zweifellos das Potenzial besitzen das europäische Zahlungssystem zu transformieren. Diese Veränderungen stellen sowohl eine Herausforderung, aufgrund des Risikos einer möglichen Disintermediation, dar, als auch eine Chance durch zusätzliche Anbieter mit verbesserter Expertise und Infrastruktur.

Verbraucherschutz

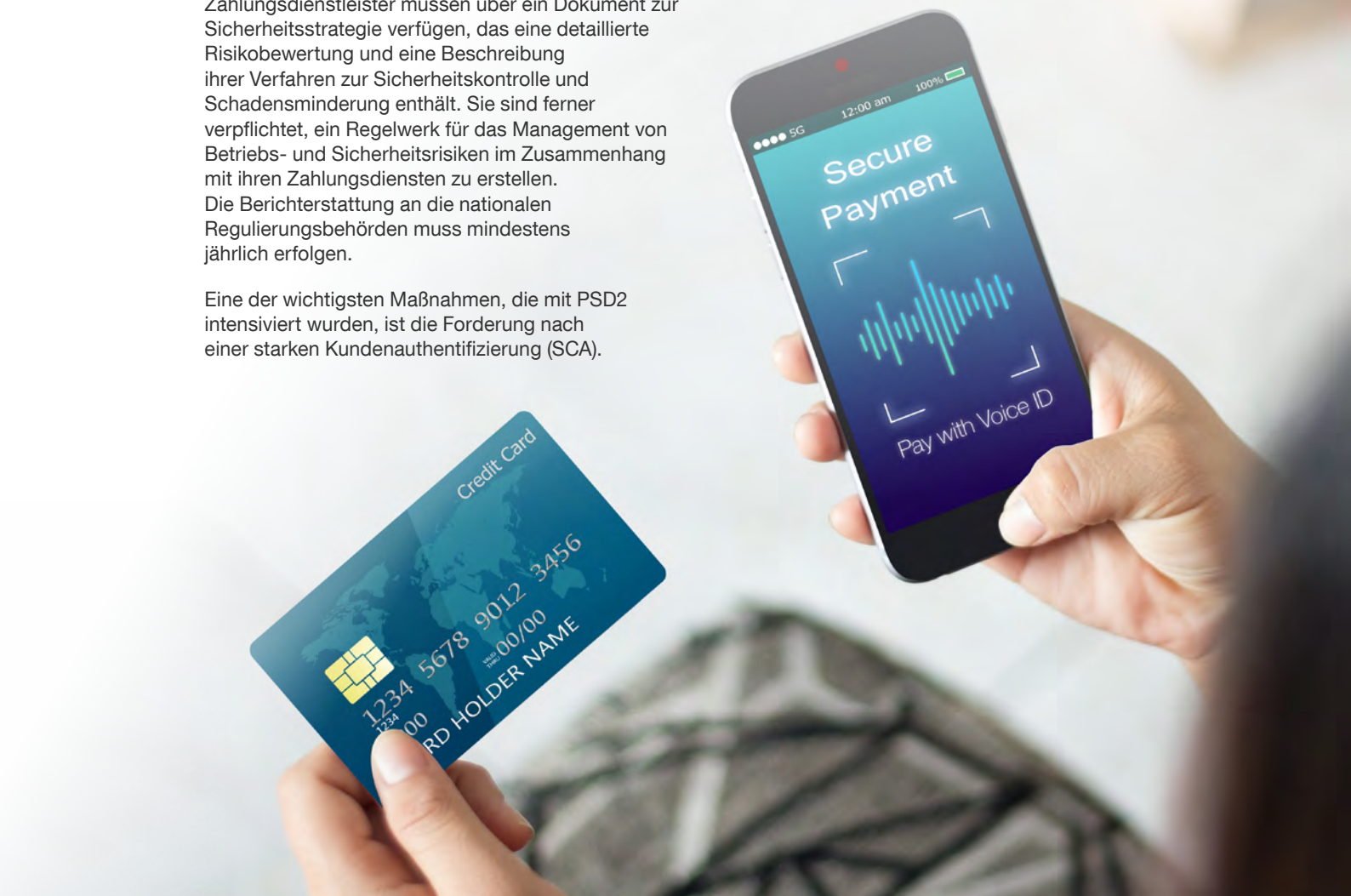
Eine gesteigerte Kostentransparenz und der Schutz vor zusätzlichen Gebühren stärken den Verbraucherschutz. Als Reaktion auf die zunehmende Internetkriminalität und den Onlinebetrug setzt PSD2 darauf, die Sicherheit bei der Zahlungsabwicklung zu verbessern. Banken bzw. Finanzdienstleister sind dann für nicht autorisierte Zahlungen verantwortlich, es sei denn, sie können nachweisen, dass der Vorgang ordnungsgemäß authentifiziert wurde und nicht von einem technischen Fehler betroffen war.

Sichere Zahlungsabwicklung

Die Sicherheitsrisiken im Zusammenhang mit dem elektronischen Zahlungsverkehr sind in den letzten Jahren gestiegen. Dies ist zum Teil auf die zunehmende technische Komplexität, die stetige Zunahme elektronischer Zahlungen sowie auf die Entwicklung neuer Zahlungsarten zurückzuführen. PSD2 überträgt den Zahlungsdienstanbietern die Verantwortung für Sicherheitsrisiken und zielt darauf ab, diese Risiken durch einen klaren und harmonisierten Rechtsrahmen zu reduzieren.

Zahlungsdienstleister müssen über ein Dokument zur Sicherheitsstrategie verfügen, das eine detaillierte Risikobewertung und eine Beschreibung ihrer Verfahren zur Sicherheitskontrolle und Schadensminderung enthält. Sie sind ferner verpflichtet, ein Regelwerk für das Management von Betriebs- und Sicherheitsrisiken im Zusammenhang mit ihren Zahlungsdiensten zu erstellen. Die Berichterstattung an die nationalen Regulierungsbehörden muss mindestens jährlich erfolgen.

Eine der wichtigsten Maßnahmen, die mit PSD2 intensiviert wurden, ist die Forderung nach einer starken Kundenauthentifizierung (SCA).



Starke Kundenauthentifizierung (SCA)

Eine der wichtigsten Säulen von PSD2 ist die starke Kundenauthentifizierung (Strong Customer Authentication, SCA); eine neue europäische Anforderung, um Onlinezahlungen sicherer zu machen und Betrug zu verhindern.

Um Zahlungen nach dem Inkrafttreten von SCA (ab 31. Dezember 2020)[3] zu akzeptieren, müssen mindestens zwei der drei folgenden Faktoren verwendet werden.

Wissen

Merkmal, das nur der Benutzer **kennt** (PIN, Passwort, usw.)

Besitz

Merkmal, das nur der Benutzer **besitzt** (Kreditkarte, RSA Token, usw.)

Inhärenz

Merkmal, das nur dem Benutzer eigen **ist** (Sprach- und Gesichtserkennung, Verhaltensbiometrie)

Zahlungsdienstleister müssen SCA einsetzen, sobald Kunden online auf ein Zahlungskonto zugreifen, eine elektronische Zahlungstransaktion einleiten sowie bei „jeder Aktivität über einen Remote-Kanal, die potenziell die Gefahr von Zahlungsbetrug oder anderem Missbrauch in sich birgt“.

Darüber hinaus müssen einige Remote-Zahlungsvorgänge – einschließlich Zahlungen über das Internet und Smartphones – die Transaktion mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger dynamisch verknüpfen und einen eindeutigen Authentifizierungscode generieren. Infolge der dynamischen Verknüpfung führt jede Änderung des Betrags oder der Identität des Zahlungsempfängers zur Ungültigkeit des Codes.

3. Die Europäische Bankenaufsichtsbehörde (EBA) hat eine Verlängerung der Übergangszeit genehmigt. Die Regelung wird erst am 31. Dezember 2020 in Kraft treten.

Auswirkungen einer starken Kundenauthentifizierung auf Finanzdienstleistungen

Die Verpflichtung zur Anwendung von SCA wirkt sich auf das gesamte Finanzwesen und insbesondere auf Finanzdienstleister aus. Die Anforderung, SCA für browserbasierte und mobile Zahlungen zu implementieren, wird deshalb zu bedeutenden Veränderungen bei den Finanzdienstleistern führen.

Um SCA zu ermöglichen, haben sich die meisten Finanzdienstleister dafür entschieden, das Senden eines Codes oder einer PIN (One Time Password, OTP) per SMS beizubehalten. **Während die Kombination von OTP per SMS (Besitzmerkmal) und dem Passwort (Wissensmerkmal), technisch die Zwei-Faktor-Regel erfüllt, setzen die Anbieter voraus, dass die von Kunden zum OTP-Empfang eingesetzten Geräte sicher sind. Die Realität sieht jedoch ganz anders aus.**

Die technischen Regulierungsstandards für starke Kundenauthentifizierung und sichere Kommunikation im Rahmen von PSD2 (Regulatory Technical Standards on strong customer authentication and secure communication under PSD2) besagen: „Die Zahlungsdienstleister stellen sicher, dass die Verarbeitung und Weiterleitung der personalisierten Sicherheitsanmeldeinformationen und der gemäß Kapitel 2 generierten Authentifizierungscodes in sicheren Umgebungen gemäß starken und weithin anerkannten Industriestandards erfolgt.“

Zunehmend verbreiteter Betrug auf der Grundlage von Kontoübernahmen und SIM-Austausch (SIM Swapping) offenbart jedoch einen deutlichen Sicherheitsmangel der im vorigen Absatz genannten Umgebungen. Dies ist ein triftiger Grund für Finanzdienstleister, die in Deutschland weit verbreitet OTP/SMS-Technologie für die Implementierung einer verbesserten Client-Authentifizierung zu verwerfen.

Finanzdienstleister wie die Postbank, die Raiffeisen Bank, die Volksbank und die Consorsbank haben ihre Absicht erklärt, OTP/SMS im Laufe des Jahres 2020 zu verbieten. Die Deutsche Bank und die Commerzbank wollen in die gleiche Richtung gehen, und viele andere werden voraussichtlich folgen.[4]

Die Verantwortung von Finanzdienstleistern im Zusammenhang mit SCA

PSD2 stellt einen wesentlichen Schritt zu mehr Verbraucherschutz bei Verlust, Diebstahl, Unterschlagung und fehlerhaften Sichherheitsmaßnahmen dar. Zahlungsdienstleistungsanbieter (Payment Service Providers, PSPs) tragen die volle Verantwortung für Zahlungen, die nicht korrekt ausgeführt wurden. Infolgedessen sind sie verpflichtet, den Gesamtbetrag der nicht autorisierten Zahlungstransaktion unverzüglich an ihre Kunden zurückzuerstatten.

Nur wenn Zahlungsdienstnutzer in betrügerischer Absicht oder aus grober Fahrlässigkeit handeln, sind diese voll haftbar.

Deshalb ist es für die Einhaltung der PSD2 von entscheidender Bedeutung, dass Finanzdienstleister eine starke und sichere Methode zur Kundenauthentifizierung implementieren. Sie muss das Risiko eines Identitätsdiebstahls minimieren, das Kundenvertrauen maximieren und gleichzeitig die betrugsbedingten Kosten weitestgehend reduzieren.

Die Konformität mit der PSD2-Richtlinie ist inzwischen eines der vorrangigen Ziele von Zahlungsdienstleistern, da Verstöße die Haftung für Betrugsschäden bei ihren Kunden zur Folge haben.

4. Article ZDNet, July 2019 – https://www.zdnet.com/article/german-banks-are-moving-away-from-sms-one-time-passcodes/

Die neue Rolle der Biometrie

Bei der Realisierung einer sicheren Kundenauthentifizierung betrachten Unternehmen die Biometrie zunehmend als optimalen Authentifizierungsansatz, da sie sowohl die Sicherheit als auch das Kundenerlebnis verbessert. Kombiniert mit einem Besitz- oder Wissens-Faktor trägt die Biometrie damit zu einer sicheren Zwei-Faktor-Authentifizierung bei.

Angesichts der Verbreitung der biometrischen Authentifizierung in vielen Smartphone- und Tablet-Geräten, wie z. B. Fingerabdruck- und Gesichtserkennung, haben sich Anwender an die Biometrie als sichere und bequeme Alternative zu Passwörtern gewöhnt.

Organisationen, die biometrische Verfahren zur sicheren Kundenauthentifizierung einsetzen wollen, müssen dabei die folgenden Überlegungen berücksichtigen:

- **Nutzung nativer biometrischer Authentifizierung vs. nicht-nativer biometrischer Methoden:** Native biometrische Authentifizierungsmethoden, die in alltäglichen Mobilgeräten integriert sind, erleichtern zwar die Nutzung, doch bietet die eingesetzte Gerätetechnologie oftmals nur eingeschränkte Sicherheit, Genauigkeit und Schutz vor Angriffen. Nicht-native Gerätetechniken ermöglichen es Organisationen, ungeachtet des Geräteherstellers oder -modells, eine konsistente Sicherheit und Anwendererfahrung zu bieten. Darüber hinaus bieten diese Methoden (je nach Biometrie-Anbieter) in der Regel ein höheres Maß an Genauigkeit sowie Anti-Spoofing-Fähigkeiten.
- **Geräteseitige vs. serverseitige biometrische Verarbeitung:** Bei der geräteseitigen biometrischen Verarbeitung verbleiben die biometrischen Daten im Gerät und Unternehmen müssen die Erfassung, Verarbeitung und den Abgleich nicht verwalten. Die serverseitige biometrische Verarbeitung ermöglicht jedoch die Verwendung derselben biometrischen Daten über mehrere Kanäle hinweg. So können z. B. „Stimmabdrücke“ sowohl bei einer Mobile-Banking-Anwendung als auch bei Anfragen im Kundenservice verwendet werden. Darüber hinaus bietet die serverseitige biometrische Registrierung einen höheren Betrugsschutz.
- **Wahl der biometrischen Verfahren:** Passive Verfahren, wie z. B. die Verhaltensbiometrie, werden als reibungslose, unsichtbare und effektive Methoden zur kontinuierlichen Authentifizierung in Web- und Mobilkanälen immer beliebter. Darüber hinaus werden vertraute und praktische biometrische Verfahren bevorzugt, die auf Geräte-Sensoren für Gesichts-, Stimm- und Fingerabdruck zurückgreifen.
- **Geeignete Kanäle:** Während PSD2 in erster Linie elektronische Transaktionen abdeckt, ist es wichtig, die Biometrie-Implementierung in einem breiteren Rahmen zu betrachten. Nur so können die Vorteile einer Omni-Channel-Lösung über digitale Kanäle, Contact Center und das stationäre Filialnetz gleichermaßen genutzt werden.

Wie kann Nuance unterstützen

Die Biometrie-Lösungen von Nuance unterstützen Sie bei der Umsetzung der PSD2- und SCA-Vorgaben, indem sie die Sicherheit der Authentifizierungs- und Betrugspräventionsprozesse erhöhen und gleichzeitig das Kundenerlebnis und die Markenbindung steigern.

Unternehmen müssen die goldene Mitte zwischen drei Zielen finden:

1. Optimierung der Kundenzufriedenheit und Maximierung der Akzeptanz authentischer Transaktionen.
2. Minimierung von betrugsbedingten Verlusten durch Erkennen und Zurückweisen betrügerischer Transaktionen bei gleichzeitiger Vermeidung von Fehlalarmen („False Positives“).
3. Kostenreduzierung in der Betrugsbekämpfung durch Automatisierung der Betrugspräventionsmaßnahmen und Minimierung der Arbeitsbelastung der Mitarbeiter durch zuverlässige Betrugswarnungen.

Am 21. Juni 2019 erklärte die Europäische Bankaufsichtsbehörde (EBA) die Gültigkeit verschiedener Biometriemethoden als ein Faktor innerhalb der „Inhärenz“[5]-Kategorie. Damit öffnete sie die Tür zur Implementierung ausgeklügelter Kundenauthentifizierungsverfahren, die nicht von möglichen Sicherheitsmängeln in Kommunikationsinfrastrukturen abhängig sind.

Die biometrischen Lösungen von Nuance zur Kundenauthentifizierung und Betrugserkennung basieren auf KI-Algorithmen, die eine schnelle und zuverlässige Authentifizierung ermöglichen. Nuance bietet mehrere integrierte biometrische Modalitäten, hohe Genauigkeit sowie starke Anti-Spoofing- und Betrugserkennung. Darüber hinaus ermöglicht eine leistungsstarke Risiko-Engine Echtzeit-Entscheidungen auf der Grundlage verschiedener Risiko- und Erkennungssignale. Die Nuance-Lösungen basieren auf langjähriger Erfahrung in der Entwicklung und Bereitstellung von professionellen Biometrie-Engines, die über 400 Mio. Kunden auf der ganzen Welt authentifizieren und von Hunderten von Unternehmen, darunter führenden Finanzinstituten, weltweit eingesetzt werden.

Zu den biometrischen Lösungen von Nuance gehören:

Verhaltensbiometrie
Wie jede Person mit seinen Geräten interagiert, ist einzigartig. Nuance Gatekeeper analysiert biometrische Verhaltensmuster, z. B. wie schnell eine Person tippt, das Smartphone hält, den Tastendruck und die Kontaktfläche der Finger bei der Interaktion mit dem Gerät oder auch, wie sie bei der Ausführung einer Aufgabe innehält. Ändern sich diese Verhaltensweisen oder entspricht das Muster dem eines potenziellen Betrügers, sorgt Nuance Gatekeeper dafür, dass die mit der Transaktion verbundene Risikobeurteilung erhöht wird. Die Verhaltensbiometrie ist eine ideale Methode zur Stärkung der Authentifizierung und um Betrug über Web-, Mobil- und Chat-Kanäle zu reduzieren, während sie für den Kunden völlig unsichtbar ist.

Voice-Biometrie/Stimmbiometrie
Unter allen biometrischen Verfahren hat die Stimmbiometrie in den letzten Jahren einen hohen Reifegrad erreicht. Nuance ist mit mehr als 500 Kunden und 400 Mio. Stimmabdrücken weltweit führend in der Bereitstellung biometrischer Technologielösungen für den Finanzsektor.

Die Stimmbiometrie-Technologie von Nuance ist in der Lage, nach der Analyse von Hunderten von Attributen und physischen Merkmalen jedes Individuums (Stimmtrakt, Sprache, Sprachvermögen usw.) sowie der Stimmen-Charakteristik, einen Stimmabdruck zu erstellen, der die Überprüfung der Identität des Sprechers mit einer Genauigkeit von über 99% gewährleistet.

Der Stimmabdruck kann zur Identifizierung des Sprechers sowohl auf einem Sprachkanal (IVR und Contact Center) als auch auf digitalen Kanälen (mobile App, Web, E-Mail, soziale Netzwerke usw.) verwendet werden.

Gesichtserkennung
Der Einsatz der Gesichtserkennung ist inzwischen weit verbreitet. Sie bietet dem Benutzer eine unkomplizierte Authentifizierungsmöglichkeit, indem sie die hochwertigen, in den meisten Smartphones und Tablets integrierten Kameras nutzt. Die Gesichtserkennung kann zudem auf Betrüger abschreckend wirken und senkt die Wahrscheinlichkeit, dass Kriminelle den Betrugsversuch fortzusetzen, wenn sie mit einer solchen Authentifizierungsanfrage konfrontiert werden. Nuance Gatekeeper bietet die Gesichtserkennung als eine Methode zur sicheren Kundenauthentifizierung und damit ein Höchstmaß an Genauigkeit.

ConversationPrint™
ConversationPrint™ ist eine Form der Verhaltensbiometrie und eine echte Branchenneuheit. Sie kann betrügerische Aktivitäten in Echtzeit auf der Grundlage von Wortwahl und Sprachmustern bzw. getipptem Text über alle Kanäle hinweg identifizieren – sowohl während einer Interaktion mit einem Menschen als auch mit virtuellen Assistenten. Durch die Analyse von Vokabular, Satzstruktur, Grammatik und mehr ermöglicht ConversationPrint™ eine kontinuierliche Authentifizierung während eines Gesprächs, z. B. in einer Chat-Sitzung. Es stellt auch eine leistungsfähige Methode zur Betrugserkennung dar, indem es Gesprächsmuster erkennt, die dem eines potenziellen Betrügers ähneln.

Mit diesen multimodalen professionellen Biometrie-Funktionen auf KI-Basis können Sie eine starke Kundenauthentifizierung umsetzen. So erreichen Sie Ihre Compliance-Vorgaben, optimieren das Kundenerlebnis und reduzieren Betrug über alle Kundeninteraktionskanäle hinweg.

5. „Inhärenz beinhaltet Techniken wie Netzhaut-, Iris- und Fingerabdruck-Scanning, Venenerkennung, Gesichts- und Handgeometrie sowie Spracherkennung“. Europäische Bankenaufsichtsbehörde (21. Juni 2019)

Nuance Intelligent Detectors
Intelligente Detektoren liefern Risiko-Signale, die die Identifizierung von Betrügern erheblich erleichtern.

Liveness ID
Stellt sicher, dass hinter den gelieferten biometrischen Daten ein Mensch steckt.

Synthetic ID
Erkennt selbst perfekt generierte synthetische Sprache.

Playback ID
Entdeckt, wenn ein Betrüger eine Tonaufnahme der Stimme seines Opfers benutzt.

Geo ID
Identifiziert das Land und die Stadt, mit denen das Gerät verbunden ist.

Network ID
Analysiert die Netzwerkqualität, um verdächtige Änderungen zu erkennen.

Channel ID
Analysiert den gesamten Audio-inhalt, um den bei der Interaktion verwendeten Gerätetyp zu erkennen.

ANI ID
Analysiert die Metadaten eines Telefongesprächs und bestimmt, wann ein eingehender Anruf von einem legitimen Anrufer stammt.

Warum Nuance?

Nuance Communications (NASDAQ: NUAN) ist ein multinationales Unternehmen mit über 30 Jahren Erfahrung in Innovation, Forschung, Entwicklung und Kommerzialisierung von biometrischen Lösungen und Technologien zum Verstehen von Stimme und natürlicher Sprache mittels künstlicher Intelligenz (KI). Viele Nuance-Lösungen sind heute im Kundenservice zahlreicher internationaler Unternehmen präsent, schaffen Mehrwert und tragen dazu bei, die Kundenzufriedenheit und -sicherheit zu verbessern.

Weltweit authentifizieren sich mehr als 400 Mio. Menschen bei Kundendiensten mit stimmbiometrischen Lösungen von Nuance. Bislang wurden jährlich über 8 Mrd. erfolgreiche biometrische Transaktionen verarbeitet – ohne eine einzige gemeldete missbräuchliche Authentifizierung. Dadurch konnten 2 Mrd. Dollar an Betrugsschäden eingespart werden.

Zu unseren Referenzkunden, die unsere biometrischen Lösungen zur Kundenauthentifizierung und Betrugsprävention einsetzen, gehören führende Banken und Finanzdienstleister, Telekommunikationsunternehmen, Versicherungen, Handels- und Versorgungsunternehmen sowie Regierungsbehörden auf der ganzen Welt. Nachstehend finden Sie einige dieser Kunden:

Manulife · BARCLAYS · Royal Bank of Scotland · Crédit du Nord
HSBC · ING · TalkTalk For Everyone · BBVA · ANZ
USAA® · Telefónica · Santander · بنك أبوظبي التجاري ADCB
Australian Government Australian Taxation Office · ROGERS · Eastern Bank · VIRGINIA Credit Union
LLOYDS BANK · Vanguard · Deutsche Telekom · nab · TD

Erfahren Sie mehr

Weitere Informationen über diese und andere Sicherheits- und Biometrie-Lösungen zur Kundenauthentifizierung und Betrugsprävention finden Sie hier.

Wenn Sie eine Produktdemo anfordern möchten oder eine Frage haben, senden Sie bitte eine E-Mail direkt an: contact-dach@nuance.com

Über Nuance Communications, Inc.
Nuance Communications (NASDAQ: NUAN) ist Pionier und Marktführer im Bereich der dialogorientierten KI für alle Arbeits- und Lebensbereiche. Das Unternehmen liefert Lösungen, die verstehen, analysieren und reagieren, mit dem Ziel die menschliche Intelligenz zu bereichern sowie Produktivität und Sicherheit zu erhöhen. Nuance besitzt jahrzehntelange Erfahrung in der Entwicklung und Anwendung von KI und bietet Lösungen u.a. für das Gesundheits- und Rechtswesen, die Finanz- und Versicherungsbranche, Telekommunikation und Versorgungswirtschaft. Tausende von Unternehmen arbeiten mit Nuance zusammen, um engere Beziehungen und bessere Erfahrungen für Kunden und Mitarbeiter zu schaffen. Weitere Informationen finden Sie unter www.nuance.de.

NUAN-CS-0000–01-WP, 20. März 2020