Sichere Biometrie stoppt Betrug in allen Kanälen.

Machen Sie Betrüger und Identitätsdiebe mit Nuance Gatekeeper sprachlos.

Kriminelle werden stets die schwächsten Kommunikationskanäle suchen und ins Visier nehmen; egal ob es sich um die Live-Kundenbetreuung, mobile Apps, Web-Services, den Live Chat oder andere Kanäle handelt. Das macht Organisationen, die diverse Kunden-Engagement-Kanäle anbieten, zu einer attraktiven Zielgruppe für Betrüger, die dabei auf die zahlreichen Informationen zugreifen, die in den sozialen Netzwerken und dem Darknet verfügbar sind. Missbrauchsversuche, inklusive illegaler Kontoübernahmen, elektronischem Zahlungsbetrug und Identitätsdiebstahl sind ein großes und wachsendes Problem für Unternehmen und Verbraucher. Im globalen Gesamtverlust durch Identitätsdiebstahl machen die aus illegalen Kontoübernahmen resultierenden Verluste mittlerweile 28% aus.

Wie aber halten Sie die immer trickreicheren Betrüger davon ab, Ihre Organisation anzugreifen? Denn möglicherweise wissen die Betrüger bereits den Namen des Lieblingshaustiers oder den Geburtstag Ihrer Kunden. Und vielleicht sind sie sogar in der Lage, die Identität der Anrufer vorzutäuschen. Sie können allerdings nicht wie Ihre Kunden sprechen, schreiben oder sich wie sie verhalten.

Nuance Gatekeeper baut auf bewährte Methoden aus der Nuance Security Suite, um Betrug im Kundenservice zu bekämpfen. Durch die Nutzung multimodaler, biometrischer Technologie gesteuert durch künstliche Intelligenz (KI) mit zielgerichteter Betrugserkennung unterstützt Nuance Unternehmen dabei, Kriminelle zu identifizieren und Betrugsversuche im Unternehmen zu stoppen.

Die größten Vorteile

Minimieren Sie direkte finanzielle Verluste, in dem bekannte Betrüger gestoppt werden. Identifizieren Sie Betrüger, die sich bei Ihrem Kundenservice wiederholt fälschlicherweise als Kunden ausgeben, und wehren Sie diese erfolgreich ab.

Verhindern Sie erneuten Betrug – Erkennen und analysieren Sie verdächtiges Verhalten durch die Verwendung von intelligenten Detektoren in Echtzeit, um neue Betrüger zu identifizieren.

Reduzieren Sie das operative Risiko – Verbessern Sie die Zufriedenheit von Kunden und Partnern, indem Betrug verhindert wird, bevor Kunden betroffen sind und ohne dass Ihre Kundendienstmitarbeiter dafür zu Sicherheitsexperten werden müssen.

Steigern Sie die Produktivität Ihres Teams zur Betrugsbekämpfung – Solide und flexible Tools bedeuten, dass sich kleinere Teams mit mehr höherwertigen und komplexeren Betrugsvorfällen befassen können.

Unterstützen Sie die Strafverfolgung – Erfassen Sie eindeutige Beweise, um die Strafverfolgung zu unterstützen und künftige Angriffe zu verhindern.

Wie es funktioniert

Nuance Gatekeeper verwendet Stimm- und Verhaltensbiometrie in Kombination mit intelligenten Detektoren, um potentiell betrügerisches Verhalten im Kundenservice zu erkennen. Sie vergleichen den Abdruck eines bekannten Betrügers (Stimme,

~70%

des Betruges im Kundenservice wird von den gleichen Tätern verübt. Deshalb ist es eine nützliche Maßnahme, die Interaktions-Abdrücke der Betrüger auf schwarze Listen zu setzen, um diese mithilfer dieser Spuren zu stoppen .[3]

Entscheidende Faktoren

- Verluste durch Kontoübernahmen stellen bis zu 28% der Gesamtverluste aufgrund von Identitätsdiebstahl im globalen Finanzsektor dar[1]
- **Einer von 867 Anrufen** beim Kundenservice von Finanzinstituten ist ein betrügerischer Anruf (der durchschnittliche Verlust pro Konto beträgt 42.546 US-Dollar)
- **92% Zunahme** des Telefonbanking-Betrugs von 2014 bis 2015[2]
- Stimmbiometrie kann dazu beitragen, Betrugskosten per Telefon im **Kundenservice um 90% zu reduzieren**, und über den mobilen Kanal um 80%

1 Note: Statistics taken from a market study on fraud related to customer interaction in banking and financial enterprises by Infinity Research, 2015
2 FRAUD THE FACTS 2016 (Financial Fraud Action UK) https://www.financialfraudaction.org.uk/
3 Litan, Avivah. Gartner, Inc. “Preventing Fraud in the Call Center with Phone Printing and Voice Biometrics” (Forbes 2014, June 18). www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/gartnergroup/2014/06/18/preventing-fraud-in-the-call-center-with-phone-printing-and-voice-biometrics/&refURL=&referrer=#133610953584

NUANCE

Verhaltens- oder gesprächsbezogen) mit dem Abdruck während eines Anrufs. Sobald ein Betrüger anruft, werden die Kundenservice-Mitarbeiter in Echtzeit gewarnt. Außerdem analysiert der Nuance Gatekeeper den Anruf in Echtzeit, um potentielle Betrugsfälle zu erkennen, wie beispielsweise verschiedene Personen, die für das gleiche Kundenkonto anrufen.

Wichtigste Funktionen

ROI in weniger als sechs Monaten – Der ROI kann schnell durch die Erstellung von KPIs auf Basis historischer Daten ermittelt werden. Die Vorteile sind vom ersten Tag an ersichtlich, und die meisten Unternehmen erreichen den ROI in weniger als sechs Monaten.

Bekannte Betrüger werden sofort entlarvt – Bekannte Betrüger werden innerhalb der ersten Sekunden des Gesprächs entdeckt. Der Kundenservice wird sofort gewarnt, damit er in Echtzeit die entsprechenden Maßnahmen ergreifen kann.

Betrugsprävention gegen unbekannte Betrüger – Nuance Gatekeeper verwendet intelligente Detektoren, um eingehende Anrufe anhand über 100 biometrischer Faktoren zu analysieren. Bei Bedarf werden Warnungen an den Kundenservicemitarbeiter gesendet, damit das Betrugsteam in Echtzeit eingreifen kann, um den Betrug zu verhindern.

Intelligente Detektoren – einschließlich einer **Kanal-ID**, um den Kanal-Typ festzustellen, der während der Interaktion verwendet wurde, einer **Netzwerk-ID**, die die Netzwerkqualität analysiert, um verdächtige Veränderungen zu entdecken sowie einer **Geo ID**, welches das Land und die Stadt ermittelt, mit denen das Gerät verbunden ist.

Anti-Spoofing einschließlich der **ANI-ID**, die die Metadaten in einem Telefongespräch analysiert, um Widersprüche festzustellen und Manipulationen an der Telefonnummer zu erkennen, der **Synthetic-ID**, die ein breites Spektrum an synthetischen Stimmtechnologien erkennt, einschließlich derer, die von DNNs erzeugt wurden, der **Liveness-ID**, die mithilfe von Echtzeit-Tests Manipulationen an der Stimme erkennt, der **Playback-ID**, die Stimmaufnahmen anhand von Audio-Anomalien erkennt, die bei der Aufnahme und während des Wiedergabe-Prozesses entstanden sein können.

Nuance DevicePrint – nicht biometrischer Abdruck, der im Gerät erstellt wurde. Er befähigt die Plattform, Fehlanpassungen zu erkennen, die auf einen potentiellen betrügerischen Anruf hinweisen.

ConversationPrint™ – ConversationPrint™ verbessert die Ermittlungspräzision um betrügerische Handlungen, Worte, Sprach- oder Schreibmuster während der Interaktion mit einem menschlichen oder virtuellen Assistenten zu erkennen. Speech-to-Text, ein wesentliches Merkmal von Nuance, wird bei kurzen Sprachsegmenten angewendet, um das Vokabular, die Satzstruktur, die Grammatik und weitere Besonderheiten eines jeden Individuums zu analysieren.

Die Brute-Force-Betrugserkennung stellt fest, wenn ein Betrüger mehrmals anruft und dabei versucht, einen Ansprechpartner zu finden, der beeinflusst werden kann. Ist dies der Fall, wird das Betrugsteam eingeschaltet, um genauer zu prüfen, ob die Stimme auf eine schwarze Liste gesetzt werden soll, damit dieser Betrüger in Zukunft direkt gestoppt werden kann.

Verbesserte Tools zur Betrugsermittlung und Strafverfolgung – Nuance Gatekeeper ermöglicht es Betrüger auf der Watchlist zu managen, verdächtige Aufnahmen zu analysieren und Betrugswarnungen gemäß ihrer Schwere zu bewerten.

Suche in historischen Daten, um Betrug zu erkennen – Aufdeckung der Identität und Verhaltensmuster von Betrügern durch die Verwendung umfangreicher historischer Suchfunktionen.

Keyword Spotting (KWS), um potentiellen Betrug herauszustellen – Das Betrugsteam kann das KWS befähigen, spezifische Wortreihen in einem Gespräch zu finden. Hierfür werden zum Beispiel Sätze wie “Ich möchte x € von meinem Sparkonto zu dieser Kreditkarte bewegen” oder “Ich möchte meine Adresse ändern” aufgezeichnet und im Verdachtsfall verglichen. So kann die Zeit, die sich das Team mit potentiellen Betrügern befassen muss, maßgeblich verringert werden.

Die marktführende Anwendung von Nuance liefert eine hochmoderne Technologie zur Betrugserkennung und Authentifizierung, die nahtlos auf einer gemeinsamen Plattform arbeitet, um finanzielle Verluste zu minimieren.

Für weitere Informationen über die Sicherheitslösungen und die Biometrie von Nuance besuchen Sie bitte https://www.nuance.com/de-de/omni-channel-customer-engagement/security.html

Über Nuance Communications, Inc.
Nuance ist Pionier und Marktführer im Bereich dialogorientierter KI-Innovationen, die Intelligenz in die tägliche Arbeit und das tägliche Leben bringen. Das Unternehmen liefert Lösungen, die verstehen, analysieren und auf Menschen reagieren, um die menschliche Intelligenz zu verstärken und Produktivität und Sicherheit zu erhöhen. Mit jahrzehntelanger Erfahrung in KI arbeitet Nuance weltweit mit Tausenden von Unternehmen aus Gesundheitswesen, Telekommunikation, Finanzdienstleistungen, Behörden und Einzelhandel zusammen, um eine intelligentere, vernetztere Welt zu ermöglichen.

NUAN–CS–3016–02–DS-GER, Nov 18 2019