NUANCE

Wie soziale Disruption Betrug im Contact Center fördert

Setzen Sie sich mit stärkeren Identitäts- und Glaubwürdigkeitsprüfungen zur Wehr.

Von Simon Marchand, CFE, Adm.A.
Chief Fraud Prevention Officer, Nuance Communications

Inhaltsverzeichnis

In Krisenzeiten reagieren professionelle Betrüger schnell. Sie spielen mit den Ängsten der Öffentlichkeit, nutzen überlastete Systeme und die Gunst der Stunde aus, um verdächtige Verhaltensweisen zu verschleiern.

80% der zertifizierten Spezialisten zur Betrugsbekämpfung[1] sagen: Das Betrugsniveau steigt in Zeiten wirtschaftlicher Not.

Allerdings sind professionelle Betrüger nicht die einzige Bedrohung für Unternehmen, die sich zusätzlich in extremen Situationen um den Eigen- und Kundenschutz sorgen. Soziale und wirtschaftliche Konflikte schaffen zudem ganz neue Bedrohungsansätze.

Angesichts neuer Herausforderungen und neuer Gegebenheiten verstoßen selbst vertrauenswürdige Mitarbeiter mitunter gegen Rechte und hintergehen das Unternehmen, für das sie arbeiten – etwa durch den Einsatz der im Firmenbesitz befindlichen persönlich identifizierbaren Informationen (PII).

68% der Täter leben entweder über ihre Verhältnisse oder haben finanzielle Schwierigkeiten.[2]

Dasselbe ist möglich bei vertrauenswürdigen Kunden. In Zeiten von Rezession und Arbeitslosigkeit können sich gesetzestreue Bürger motiviert sehen, freundlichen" Betrug zu begehen oder falsche Versicherungsansprüche zu stellen.

In diesem Whitepaper beleuchten wir, wie sich eine derartige Betrugswelle auf Contact Center auswirken kann. Ferner betrachten wir, wie manche CX-Manager aufkommende Authentifizierungstechnologien wie Biometrie und Glaubwürdigkeitsprüfung nutzen, um Kunden und Unternehmen in schwierigen Zeiten wirk-samer zu schützen.

Fallbeispiel: COVID-19

400% Anstieg der Betrugsversuche bei einer Privatkundenbank während des Ausbruchs.[3]

$24M Geschätzte Betrugskosten in Verbindung mit COVID-19 in den USA Januar - April 2020.[4]

$500K Geschätzter täglicher Verlust aufgrund von Betrug im Zusammenhang mit COVID-19 seit April 2020 (nur USA).[5]

Wie soziale Disruption Betrug im Contact Center fördert

Rapider wirtschaftlicher Abschwung, einschneidende Veränderungen der Lebens- und Arbeitsbedingungen – Zeiten der Unruhe erhöhen die Belastung für Contact Center und ihre Mitarbeiter.

Unter diesen Bedingungen wächst auch Betrug. So werden die ohnehin schon stark belasteten Contact-Center-Leiter zusätzlich mit zunehmenden betrügerischen Aktivitäten an drei verschiedenen Fronten konfrontiert.

Bedrohung durch professionelle Betrüger

Die COVID-19-Pandemie von 2020 zeigt, dass sich soziale Disruption durch plötzlich gestiegene Kommunikationsspitzen zwischen Menschen und den Organisationen, von denen sie abhängig sind, bemerkbar macht.

Kunden benötigen mehr Rat und Unterstützung, um Zahlungen aufzuschieben, Soforthilfe zu beantragen, Buchungen zu stornieren und ihre Bestände zu überprüfen. Wirken sich die Folgen der Krise auf den regulären Betrieb von stationären Geschäften und Contact Center aus, so verschiebt sich das Verhältnis zwischen Anrufen und verfügbaren Agenten sprunghaft.

Das Resultat ist ein ideales Umfeld für professionelle Betrüger.

In ID- und Authentifizierungsprozessen entstehen Risse

Angesichts solch überwältigender Nachfrage sind Agenten eher geneigt die durchschnittliche Bearbeitungszeit (Average Handle Time, AHT) über ein ordentliches Vorgehen zu stellen, und die Maßnahmen zur Identitätsüberprüfung weniger rigoros und konsequent anzuwenden als üblich.

Social Engineering hat mehr Aussicht auf Erfolg

Servicemitarbeiter arbeiten möglicherweise im Homeoffice ohne direkte persönliche Unterstützung und Unterweisung durch Kollegen und Vorgesetzte. Gleichzeitig sind sie bemüht, sich mit neuen Kundenfragen, neuen Produkten und neuen Verfahren auseinanderzusetzen, die alle durch die Krise verur-sacht wurden.

Demzufolge wird es wahrscheinlicher, dass sie korrekte Vorgehensweisen nur antizipieren und damit anfälliger für Social Engineering werden, womit Kriminelle persönlich identifizierbare Informationen (PII) versuchen zu stehlen.

Betrügerisches Verhalten wird immer schwerer erkennbar

In turbulenten Zeiten ändert sich das, was normales Verhalten ausmacht. Seriöse Kunden fangen an, sich ungewöhnlich zu verhalten. In Kombination mit der all-gemeinen Zunahme von Kundenkontakten kann dies zu einer Rekord-Arbeitsbelastung für das eingesetzte Team zur Betrugsbekämpfung führen. Das bedeutet auch, dass mehr Betrugsfälle länger unentdeckt bleiben.

Warum während Umwälzungen Betrugstrends je nach Industriezweig variieren

Betrug ist das Geschäft des professionellen Kriminellen. Und wie bei jedem anderen können Perioden der Unruhe und Krisen sie dazu zwingen, den Schwerpunkt ihrer Aktivitäten zu ändern. Daraus entstehen unterschiedliche Betrugstrends in verschiedenen Branchen.

Wenn beispielsweise soziale Spannungen mit einem Lockdown einhergehen, wird es schwieriger, Anmeldebetrug bei Telekommunikationsunternehmen zu begehen, weil Läden geschlossen und Geräte schwieriger zu manipulieren sind.

Stattdessen konzentrieren geschickte Betrüger ihre Ressourcen darauf, Banken anzugreifen und sich dabei ihr Wissen zunutze zu machen, wann genau Sonderzahlungen für Hilfsleistungen die Konten der Bürger erreichen.

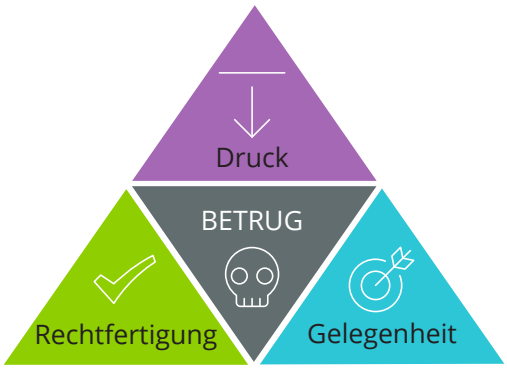
9 von 10

Fachleuten im Bereich der Betrugsbekämpfung sagen voraus, dass in den auf den April 2020 folgenden 6 bis 12 Monaten diese Effekte häufiger auftreten werden.[6]

- Betrug bei Hilfsorganisationen und Spendenaktionen
- Phishing durch Identitätsfälschung bei Behörden und Gesundheitsämtern
- Cyberangriffe im Zusammenhang mit Heimarbeit

Bedrohung durch neue Akteure

Gelegenheit. Motivation. Rechtfertigung. Dies sind die drei Seiten des klassischen „Betrugs-Dreiecks“ laut dem Kriminologen Donald Cressey. Diese Hypothese beschäftigt sich mit der Frage, was ein vertrauenswür-diger Mitarbeiter vorfinden muss, um gegen das in ihn gesetzte Vertrauen zu verstoßen und betrügerisch tätig zu werden.



Das Betrugs-Dreieck
In Zeiten sozialer und wirtschaftlicher Krisen steigen sowohl die Gelegenheiten als auch der finanzielle Druck für Contact-Center-Agenten und die von ihnen betreuten Kunden.

Ehemals vertrauenswürdige Agenten

Für Contact-Center-Agenten können soziale Konflikte zu einer dramatischen Veränderung des Arbeitsrhythmus und der Arbeitsumgebung führen. Sie werden von Kollegen und ihrer gewohnten Umgebung getrennt, aus dem Blickfeld der Vorgesetzten gerückt und es ist praktisch unmöglich, eine „Clean-Desk-Policy“ durchzusetzen.

Jede Krise, die zu weitreichenden Arbeitsplatzverlusten führt, übt einen enormen finanziellen Druck auf Einzelpersonen und Haushalte aus. In dem Maße, wie Agenten merken, dass sie sich mit neuen BBetrugsmöglichkeiten „absichern können“, entwickeln sie und ihre Familien gegebenenfalls auch die entsprechende Motivation dazu.

Gleichzeitig sind Audit- und Compliance-Abteilungen die ersten, bei denen in wirtschaftlich schwierigen Zeiten Sparmaßnahmen eingesetzt werden, was die interne Betrugsabwehr weiter schwächt.[7]

93% **der Experten für Betrugsbekämpfung** rechnen damit, dass der Betrug bei staatlichen Konjunkturprogrammen bis Oktober 2020 bzw. April 2021 zunehmen wird.[9]

86% **der Experten für Betrugsbekämpfung** rechnen damit, dass der Betrug im Zusammenhang mit Arbeitslosengeld bis Oktober 2020 bzw. April 2021 zunehmen wird.[10]

Druck ist die treibende Kraft
Studien zu der durch die Finanzkrise bedingten Rezession (2007-2009) deuten darauf hin, dass in schwierigen Zeiten Druck der Haupttreiber für Betrug am Arbeitsplatz ist.

In einer Umfrage der Association of Certified Fraud Examiners (ACFE) identifizierte fast die Hälfte (49,1 %) der befragten Experten Druck als den primären Faktor, der zu einem Anwachsen der Kriminalität führt. Als zweithäufigste Antwort wurden erhöhte Chancen von 27,1 % der Befragten genannt.

Ein Finanzinstitut sah einen

2X so hohen Anstieg der Betrugsversuche durch rechtmäßige Kontoinhaber während der COVID-19-Pandemie.[11]

Ehemals vertrauenswürdige Kunden

In einer Zeit öffentlicher Krisen oder eines wirtschaft-lichen Abschwungs stehen die Kunden, die mit Contact-Center-Agenten sprechen, oft selbst unter finanziellem Druck.

Viele von ihnen müssen mitunter finanzielle Einbußen durch ein vermindertes Einkommen in Kauf nehmen. In anderen Fällen haben sie vielleicht mit unerwarteten Gesundheitsausgaben zu kämpfen. Ähnlich wie Agenten könnten auch sie feststellen, dass Gelegenheiten zum betrügerischen Verhalten wachsen, z. B. wenn Regierungen neue Programme zur Unterstützung der

besonders Betroffenen einführen. Unter derartigen Umständen können auch vertrauenswürdige Kunden die Hemmschwelle überschreiten und im eigenen Namen betrügerische Handlungen begehen, etwa:

— Falsche Ansprüche bei Versicherungen geltend machen.

— Beantragung von finanziellen Hilfen, auf die sie keinen Anspruch haben.

— Anfechtung von Kreditkartentransaktionen nach Erhalt von Waren/Dienstleistungen.

Möglichkeiten zur Betrugsbekämpfung

Wie können CX-Manager das erhöhte Betrugsrisiko bekämpfen, das sowohl von professionellen Kriminellen als auch von Beschäftigten und Bürgern ausgeht, die zu kriminellen Handlungen motiviert werden?

Genau wie in Zeiten relativer Stabilität sollte jede umfassende Schadensbegrenzungsstrategie neben technologischen auch kulturelle und verfahren-stech-nische Maßnahmen umfassen. Organisationen, die z. B. regelmäßige Gespräche mit Agenten im Homeoffice führen oder gar Mitarbeiterberatung anbieten, stärken nicht nur die Widerstandskraft ihrer Mitarbeiter gegenüber Social Engineering, sondern minimieren auch die Wahrscheinlichkeit, dass sie selbst kriminell aktiv werden.[12]

Im folgenden Teil dieses Whitepapers konzentrieren wir uns auf Technologien, die zur Minimierung der Betrugsmöglichkeiten beitragen und bei der Identifizierung möglicher Betrüger helfen.

Bekämpfung professioneller Betrüger mit Biometrie

Biometrische Lösungen sind eine Alternative zur wissensbasierten Authentifizierung. Statt der Frage eines Agenten nach persönlich identifizierbaren Informationen (PII) eines Kunden oder dessen Kennwort wird dieser anhand eines für ihn eindeutigen Merkmals identifiziert, z. B. seiner Stimme oder der Art und Weise, wie er in die Tastatur tippt.

„Jetzt ist es für Organisationen an der Zeit, ihre internen Kontrollen zu verstärken“
Dorris, Präsident des ACFE, in seinem Artikel „Coronavirus Pandemic Is a Perfect Storm for Fraud“[13]

Wie die HSBC in UK Betrug mit Biometrie bekämpft
In einem Artikel im Biometric Update vom März 2020 wird beschrieben, wie die HSBC mit dem stimmbiometrischen System VoiceID 493 Millionen US-Dollar vor Betrügern schützen konnte.

Wie Kerri-Anne Mills, Head of Contact Centre and Customer Service bei HSBC UK, erklärte, setzt das Unternehmen biometrische Daten ein, um seine Kunden zu authentifizieren und Betrüger proaktiv zu identifizieren:

„Inzwischen verzeichnen wir jede Woche rund 16.000 Kunden über VoiceID und die Technik wird weiterhin eine zentrale Rolle bei der Betrugsbekämpfung spielen. Sie erstellt eine Bibliothek mit Stimmabdrücken von Betrügern und gleicht diese mit neu eingehenden Anrufen ab.“[14]

Da Kundenpasswörter und PII einfacher im Dark Web zu erwerben sind und sich Unternehmen verstärkt auf die Optimierung der Nutzer- und Agenten-Erfahrung konzentrieren, wird die biometrische Authentifizierung immer beliebter.

In Zeiten des sozialen Umbruchs bringt die Biometrie darüber hinaus zusätzliche Vorteile – nicht zuletzt im Kampf gegen professionelle Kriminelle, die versuchen, außergewöhnliche Umstände auszunutzen.

Den Druck auf Agenten verringern
Steigt das Anrufvolumen und sinken die Kapazitäten, machen Agenten leicht Fehler. Die Stimmbiometrie befreit die Agenten von der Pflicht, wissensbasierte Authentifizierungsfragen zu stellen, und hilft so dabei, lange und schwierige Gespräche mit legitimierten, unter Stress stehenden Kunden zu verkürzen.

PII von Agenten-Bildschirmen verbannen
Wenn Contact-Center-Agenten die PII eines Kunden nicht mehr einsehen müssen, um dessen Identität zu authentifizieren, haben Betrüger äußerst begrenzte Möglichkeiten, sich personenbezogene Daten für den ID-Diebstahl oder -Verkauf zu beschaffen.

Aktive Identifizierung bekannter Betrüger
Genauso wie legitimierte Kunden können auch professionelle Kriminelle aktiv durch ihre Stimme oder ihr Verhalten identifiziert werden. So wird die Stimme eines Anrufers mit einer Datenbank der Stimmabdrücke bereits bekannter Betrüger biometrisch analysiert.

Kommt es zu einer Übereinstimmung, wird der Anruf für weitere Sicherheitsüberprüfungen registriert, wodurch Social-Engineering- und Betrugsversuche erfolgreich verhindert und die Arbeitsbelastung des Teams zur Betrugsprävention minimiert werden kann.

Neuartige Betrüger durch biometrische Authentifizierung und Glaubwürdigkeitsüberprüfung verhindern

Die Einführung bzw. Ausweitung biometrischer Authentifizierungsprogramme kann für Verantwortliche von Contact Centern, eine wirksame Strategie zur Prävention krimineller Handlungen sein. Die Identifizierung unseriöser Kunden, die zu betrügerischem Handeln motiviert sind, erfordert jedoch einen ganz anderen Ansatz. Die Glaubwürdigkeitsauthentifizierung arbeitet genau daran.

Um zu verstehen, wie sich die Glaubwürdigkeitsauthentifizierung in die Methoden der Betrugsprävention einfügt, nehmen wir das Beispiel eines Kunden, der das Contact Center seines Versicherers anruft:

Authentifizierungssystem des Versicherers die Stimme des Kunden und bestätigt seine Identität. Im weiteren Verlauf des Gesprächs analysiert das System zur Glaubwürdigkeitsauthentifizierung die Sprache des Kunden. Das System bestätigt, dass er so spricht, wie jemand mit einem echten Versicherungsanspruch sprechen würde, und dass er keine Anzeichen dafür zeigt, den Agenten täuschen zu wollen.

Wenn das System aber annimmt, dass der Kunde unredlich handelt, kann dessen Anspruch sofort zur weiteren Untersuchung markiert werden.

Persönlich identifizierbare Informationen (PII) und damit verbundene Gelegenheiten verringern
Biometrische Authentifizierung vermindert die Anzahl der Agenten, die für die Bearbeitung von Kundenanfragen Zugriff auf PII benötigen. Dadurch werden Möglichkeiten, solche Informationen zu monetarisieren oder Identitätsdiebstahl zu begehen, erheblich eingeschränkt.

Erkennen, wann Kunden gegen das Gesetz verstoßen
Die Glaubwürdigkeitsauthentifizierung hilft zu erkennen, wenn vertrauenswürdige Kunden unehrlich handeln, und bietet eine nützliche Kontrollmöglichkeit gegen falsche Ansprüche und „freundlichen" Betrug.

Wie große Versicherer und Banken mit Glaubwürdigkeitsauthentifizierung gegen Betrug vorgehen
Glaubwürdigkeitsauthentifizierung ist zwar eine vergleichsweise neue Disziplin, aber sie entwickelt sich rasant weiter.

86 % Treffergenauigkeit laut Aussagen einer US-amerikanische Bank

Flexibilität bei der Betrugsbekämpfung mit KI
Sowohl biometrische Systeme als auch solche zur Glaubwürdigkeitsauthentifizierung beruhen auf KI und nicht auf Personal und Fachwissen. Daher lassen sie sich im Falle sozialer Disruption schnell skalieren und ausweiten, um die steigende Zahl der Betrugsversuche zu verringern.

Erste Schritte zur Betrugsbekämpfung in schwierigen Zeiten

Wenn sich unsere Welt verändert, blüht der Missbrauch. Deshalb müssen Contact-Center- und CX-Manager verstehen, wie soziale Umwälzungen zu Betrug führen, und wie sie sich darauf vorbereiten können.

Das bedeutet jene Umfelder, Prozesse und Lösungen zu identifizieren und zu fördern, die nicht nur den Betrug während des täglichen Ablaufes minimieren, sondern auch Möglichkeiten und Motivation, die mit außergewöhnlichen Umständen einhergehen.

Eine der besten Möglichkeiten, auf Betrugsversuche vorbereitet zu sein, ist es, mit Fachkollegen zu sprechen, die vor vergleichbaren Herausforderungen stehen.

Simon Marchand ist Chief Fraud Prevention Officer bei Nuance. Neben seinen eigenen Erfahrungen und Fachkenntnissen kann er Sie mit Contact-Center- und CX-Managern anderer Organisationen zusammenbringen, um gemeinsame Herausforderungen zu diskutieren und neue Lösungen zu finden.

Simon Marchand, CFE, Adm.A.
Chief Fraud Prevention Officer, Nuance Communications

Simon Marchand

besitzt mehr als zehn Jahre Erfahrung in der Betrugsbekämpfung im Bankenwesen und in der Telekommunikation. Vor seiner Tätigkeit bei Nuance arbeitete er in Schlüsselpositionen im Betrugsmanagement bei der in Montreal ansässigen Laurentian Bank, bei Bell Canada und war professioneller Prüfer im Auftrag von Québecs Chartered Administrators.

SPRECHEN SIE UNS AN

Weitere Informationen zur Betrugsbekämpfung in schwierigen Zeiten erhalten Sie auf unserer Homepage oder per E-Mail unter contact-dach@nuance.com.

1 Quelle: https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
2 Quelle: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf
3 Quelle: Nuance-Kunde
4 Quelle: https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints.pdf, abgerufen am 6. Mai 2020.
5 Quelle: https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints.pdf, abgerufen am 6. Mai 2020.
6 https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
7 Quelle: https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
8 Quelle: https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/occupational-fraud.pdf
9 Quelle: https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
10 Quelle: https://www.acfeinsights.com/acfe-insights/covidfraudsurvey
11 Quelle: Nuance-Kunde
12 Quelle: https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/occupational-fraud.pdf
13 Quelle: Coronavirus Pandemic Is a Perfect Storm for Fraud – https://www.acfeinsights.com/acfe-insights/coronavirus-pandemic-is-a-perfect-storm-for-fraud
14 Quelle: https://www.biometricupdate.com/202003/hsbc-uks-voice-biometrics-system-blocked-2x-more-fraud-attempts-in-2019

Über Nuance Communications, Inc.
Nuance Communications, Inc. (NASDAQ: NUAN) ist Technologie-Pionier und Marktführer im Bereich der dialogorientierten KI für alle Arbeits- und Lebensbereiche. 85 Prozent aller Fortune-100 Unternehmen weltweit und 90 Prozent der Krankenhäuser in den USA vertrauen Nuance als Full-Service-Partner. Wir liefern intuitive Lösungen mit dem Ziel die menschliche Intelligenz zu bereichern sowie Produktivität und Sicherheit zu erhöhen.

ENT_4075_01_WP, 22 Okt 2020_GER