Aitē PARTNER. ADVISOR. CATALYST.

Identitätsprüfung: Erfolgreiche Strategien zur Minimierung falsch positiver Ergebnisse und Risiken

JANUAR 2019

Im Auftrag von:

melissa®

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ZUSAMMENFASSUNG

Das Whitepaper *„Identitätsprüfung: Erfolgreiche Strategien zur Minimierung falsch positiver Ergebnisse und Risiken“* hat die Aite Group im Auftrag von Melissa erstellt. Es erörtert die Herausforderungen im Zusammenhang mit der Identitätsüberprüfung von Neukunden, die die Ziele von Banken in Bezug auf eine effektive Betrugsprävention und die Einhaltung der Know-Your-Customer (KYC)-Richtlinien erreicht und gleichzeitig Unstimmigkeiten in der Customer Experience minimiert.

Zu den wichtigsten Ergebnissen der Studie zählen:

- Anwendungsbetrug wird bis 2020 zu Verlusten von mehr als 2,7 Milliarden US-Dollar bei Kreditkarten- und Sichteinlagenkonten (DDA) in den USA führen.
- Mit der starken Zunahme der Bedrohungslage wächst gleichzeitig der Druck, Unstimmigkeiten in der Customer Experience zu reduzieren oder zu beseitigen. Auf die Frage nach den wichtigsten Business-Case-Treibern für Tools zur Risikobewertung von Neukunden, gaben 88 % der befragten Betrugsverantwortlichen an, dass die Verbesserung der Customer Experience beim Onboarding ein wichtiger Faktor ist.
- Infolge des eskalierenden Bedrohungsumfelds und des Wettbewerbsdrucks zur Verringerung der Unstimmigkeiten plant fast die Hälfte der Befragten, in den nächsten Jahren den Anbieter von Neukunden-Risikobewertungen zu wechseln oder weitere hinzuzufügen. Das ist ein Anstieg gegenüber 2015, als dies nur 27 % der Befragten beabsichtigten.
- Die globale Datenbank von Melissa unterstützt sowohl deterministische als auch probabilistische Matching-Strategien zur Optimierung der Matching-Routinen. Zudem verwendet Melissa leistungsfähige Link-Analysen und Entitätsauflösung für ihre eigenen Daten und die ihrer Kunden, um Dubletten zu minimieren.
- Eine wirksame Betrugsbekämpfung stellt für Finanzdienstleistungsunternehmen zunehmend ein Wettbewerbsproblem dar. Early Adopter von Technologien der nächsten Generation werden nicht nur in der Lage sein, Betrug zu reduzieren, sondern sie können zusätzlich die Customer Experience verbessern und so einen entscheidenden Vorteil gegenüber den Wettbewerbern erreichen, die bei diesen Investitionen hinterherhinken. Daten sind die neue Währung und die optimale Informationsgewinnung aus Daten kann Unternehmen einen Wettbewerbsvorsprung verschaffen.

EINLEITUNG

Zeit ist Geld, auch wenn es um die Eindämmung von Wirtschaftskriminalität geht. Die organisierte Kriminalität, die über Milliarden von kompromittierten Datensätzen verfügen, haben mit ausgeklügelten Anwendungsbetrugsangriffen systematisch und methodisch Finanzdienstleistungsunternehmen im Visier. Sie verwenden gestohlene oder gefälschte Identitäten, um neue Konten zu erhalten. Die Verlaufskurve dieser Angriffe nimmt weiter zu, da die negativen Folgen (z. B. Gefängnisaufenthalte) vergleichsweise gering sind.

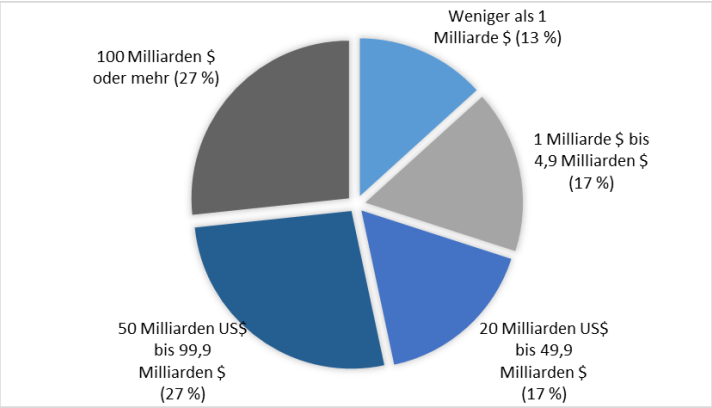
Eine der wichtigsten Herausforderungen für Führungskräfte im Bereich Betrug und Anti-Geldwäsche (AML) besteht darin, dass Finanzinstitute trotz des weiter eskalierenden Bedrohungsumfelds unter starkem Wettbewerbsdruck stehen, um das Bankgeschäft einfach und reibungslos zu gestalten. Angesichts dieser scheinbar widersprüchlichen Aufträge suchen viele Finanzinstitute nach besseren Lösungen, dass das Onboarding bei der Identitätsprüfung unterstützt.

Dieses Whitepaper behandelt die Herausforderung der Identitätsprüfung, ohne in die Customer Experience einzugreifen, sowie die operativen Auswirkungen von falsch positiven Ergebnissen. Es adressiert den Bedarf an Lösungen der nächsten Generation, die bei der Identitätsprüfung helfen, und stellt Melissas Ansatz zur Problemlösung vor.

METHODIK

Die Aite Group befragte von März bis Juni 2018 Führungskräfte amerikanischer Finanzinstitute, um die Trends bei Anwendungsbetrug sowohl in Bezug auf DDA als auch bei Kreditkarten besser zu verstehen. Die Vermögensgrößen der teilnehmenden Finanzinstitute reichen von unter 1 Mrd. $ bis über 100 Mrd. $ (Abbildung 1). Die Umfrage aktualisiert eine ähnliche Erhebung aus 2015. In diesem Whitepaper werden die beiden Daten der beiden Befragungen verglichen.

Abbildung 1: Vermögensgröße der befragten Finanzinstitute



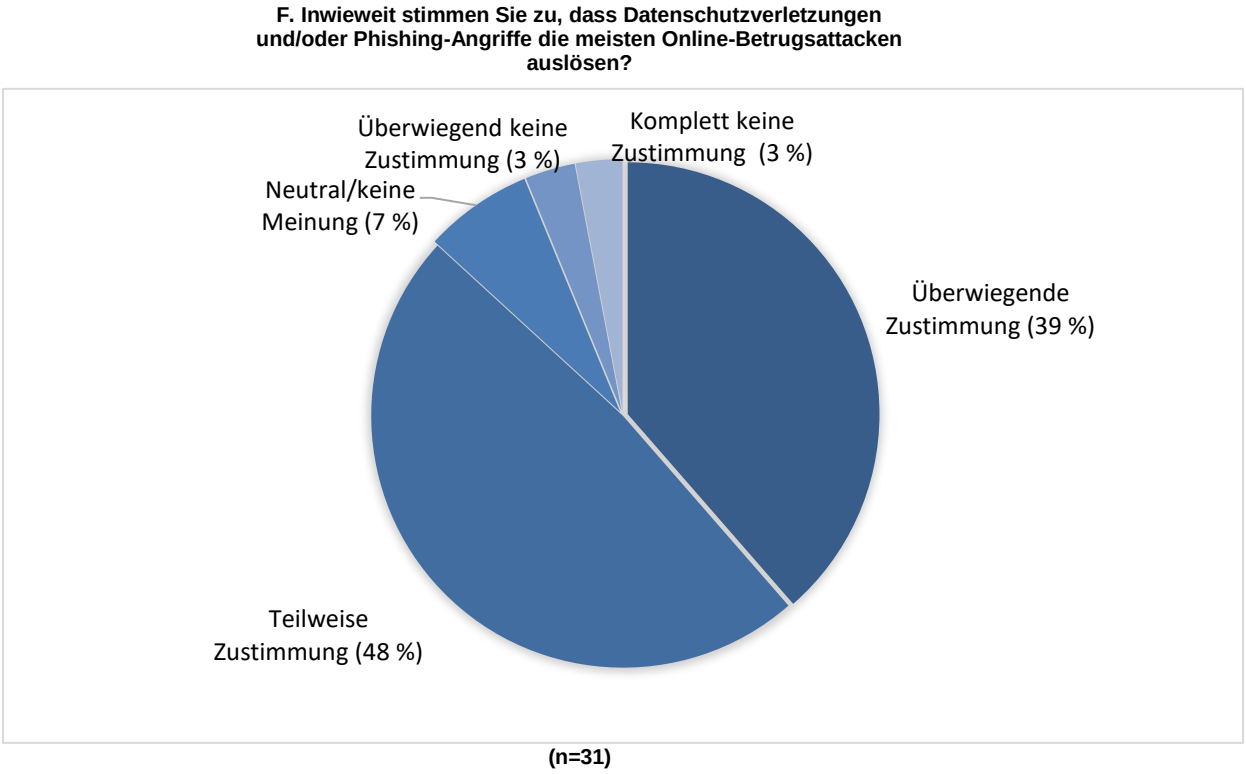
Quelle: Umfrage der Aite Group unter 30 FI, März bis Juni 2018

Das Whitepaper stützt sich ferner auf eine Umfrage der Aite Group unter 32 Führungskräften in den USA, die für die Bekämpfung von Finanzkriminalität zuständig sind. Diese wurde im September 2018 durchgeführt und behandeltet Probleme und geplante Technologieausgaben. Alle Bank-Teilnehmer dieser Umfrage kamen aus größeren Instituten mit einem Vermögen von mehr als 30 Milliarden $. Angesichts der Größe und Struktur der Forschungsstichproben liefern die Daten einen richtungsweisenden Hinweis auf die Marktbedingungen.

HERAUSFORDERUNGEN VON IDENTITÄTSÜBERPRÜFUNGEN

Mit mehr als 13 Milliarden gestohlenen oder verlorenen Datensätzen seit 2013 verfügt das organisierte Verbrechen über reichlich Material, um ihre Angriffe auf das Ökosystem der Finanzdienstleistungen voranzutreiben.[1] Die Auswirkungen der Datenschutzverletzungen sind beträchtlich. 87 % der von der Aite Group befragten Führungskräfte, die für die Bekämpfung von Finanzkriminalität zuständig sind, glauben, dass Datenverstöße oder Phishing-Angriffe für den Großteil des Betrugs auf digitaler Ebene verantwortlich sind (Abbildung 2).

Abbildung 2: Auswirkungen von Datenverstößen auf Betrugsraten

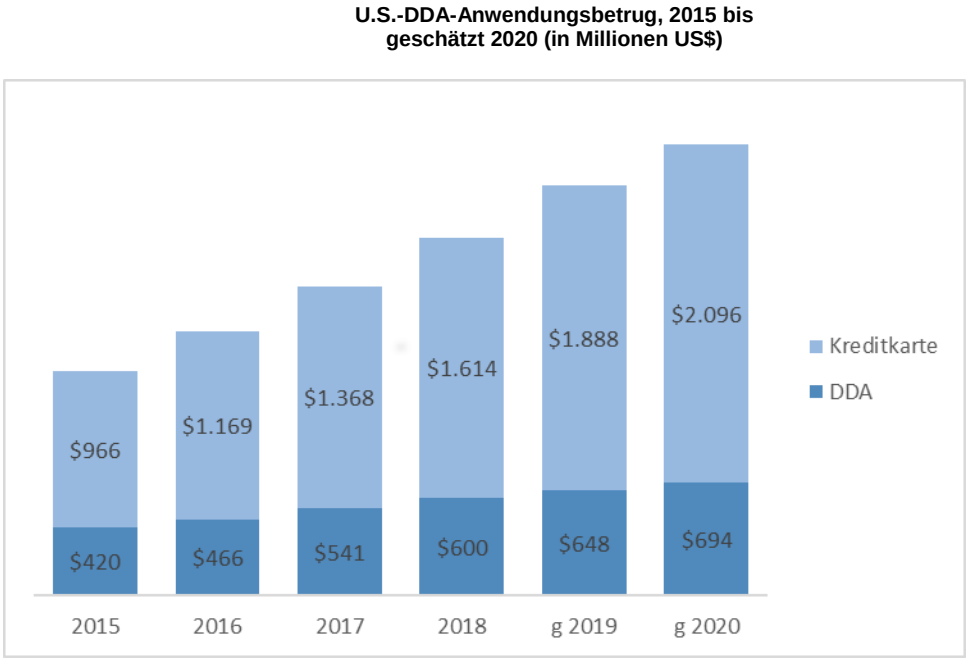


Quelle: Umfrage der Aite Group unter 32 Führungskräften, zuständig für die Bekämpfung von Finanzkriminalität, September 2018

Anwendungsbetrug äußert sich in Form von Identitätsdiebstahl (der Angreifer nutzt die Identität des Opfers) oder in Form von künstlichem Identitätsbetrug (Betrüger erstellen entweder eine komplett neue Identität oder sammeln Bruchstücke gestohlener Daten, um eine neue Identität zu erstellen). Die kombinierten Auswirkungen dieser Angriffsmethoden werden bis 2020 in den USA zu mehr als 2,7 Milliarden $ an Kreditkarten- und DDA-Betrugsverlusten führen (Abbildung 3).

1. "Breach Level Index," Abruf am 7. Dezember 2017, http://breachlevelindex.com.

Abbildung 3: Anwendungsbetrugsverluste in den USA bis 2020



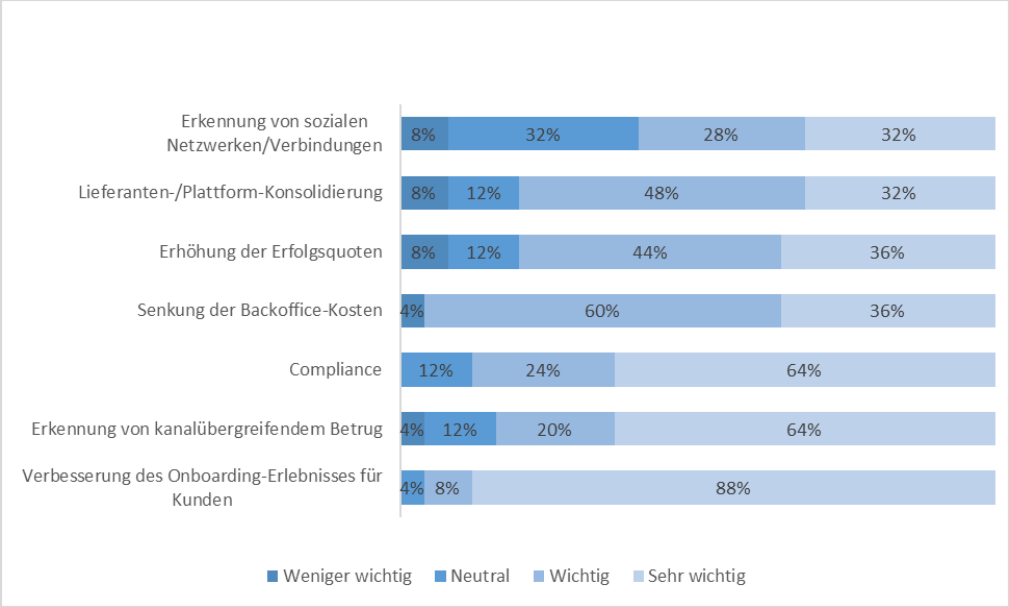
Quelle: Aite Group

Gleichzeitig mit der starken Zunahme der Bedrohungslage wächst der Druck, Unstimmigkeiten in der Customer Experience zu reduzieren oder zu beseitigen. Die Erwartungserhaltung von Verbrauchern wird dabei zunehmend durch die Erfahrungen bei Apple, Lyft und Amazon geprägt. Finanzinstitute stehen vor der Herausforderung, ähnlich reibungslose und elegante Interaktionen zu ermöglichen. Die Bedeutung der Benutzerfreundlichkeit beginnt beim Onboarding. Hier sehen Finanzinstitute nach wie vor eine hohe Fluktuation, wenn Hürden im Prozess bei potenziellen Kunden im Weg stehen.

Die Bedeutung der Customer Experience wird durch die Daten in Abbildung 4 verdeutlicht. Auf die Frage nach den wichtigsten Business-Case-Treibern für Tools zur Risikobewertung von Neukunden angesprochen, geben 88 % der befragten Führungskräfte an, dass die Verbesserung des Onboarding-Erlebnisses für Kunden ein wichtiger Business-Case-Treiber ist. Während Betrugserkennung und KYC-Compliance für 64 % der Befragten ebenfalls sehr wichtig sind, hat die Customer Experience für die Mehrheit der Befragten offensichtlich mehr Gewicht.

Abbildung 4: Faktoren, die Investitionen antreiben

F. Wie wichtig sind die folgenden Punkte bei der Bestimmung Ihrer Investitionen in Instrumente zur Risikobewertung von Neukunden? (n=25)



Quelle: Umfrage der Aite Group unter 30 FI, März bis Juni 2018

DIE HERAUSFORDERUNG BEZÜGLICH FALSCHMELDUNGEN

Die Identitätsprüfung ist ein wesentlicher Bestandteil des Onboardings neuer Bankkunden. Sie ist in KYC-Vorschriften in Ländern auf der ganzen Welt enthalten und ein notwendiger Bestandteil der Betrugsprävention bei Finanzinstituten. Die Identitätsverifizierung stellt jedoch keineswegs eine einfache Aufgabe dar. Wenn es darum geht, Unstimmigkeiten bei der Onboarding-Erfahrung zu beseitigen, ist die Reduzierung der mit der Identitätsverifizierung verbundenen Falschmeldungen ein zentraler Punkt.

In den USA gibt es keine primäre Datenquelle, um die Identität einer Person abzufragen. Stattdessen fragen Unternehmen Datenbestände ab, die auf Grundlage einer Vielzahl öffentlicher Datenquellen (z. B. Daten des U.S. Postal Service) erstellt worden sind sowie aus von gemeldeten Handelslinien (z. B. Kreditbürodaten) geschaffenen Beständen. Die Nutzung dieser sekundären Datenquellen für die Identitätsprüfung ist mit einer Vielzahl von Herausforderungen verbunden:

- Unternehmen, die an Datendepots berichten, liefern oft keine perfekten Daten – es gibt zum Beispiel Eingabefehler, alte Adressen oder Namensänderungen.
- Kunden und Mitarbeiter verursachen oft Tippfehler, so dass vielfach eine falsch eingegebene Anmeldung gegen falsch eingegebene Daten aus öffentlichen Aufzeichnungen abgeglichen wird.

- Während das Fuzzy-Matching bei Tippfehlerproblemen und bei der Identifizierung von Versuchen, Identitäten zu manipulieren, helfen kann, führt es immer wieder zu vielen Warnmeldungen, die manuell überprüft werden müssen.

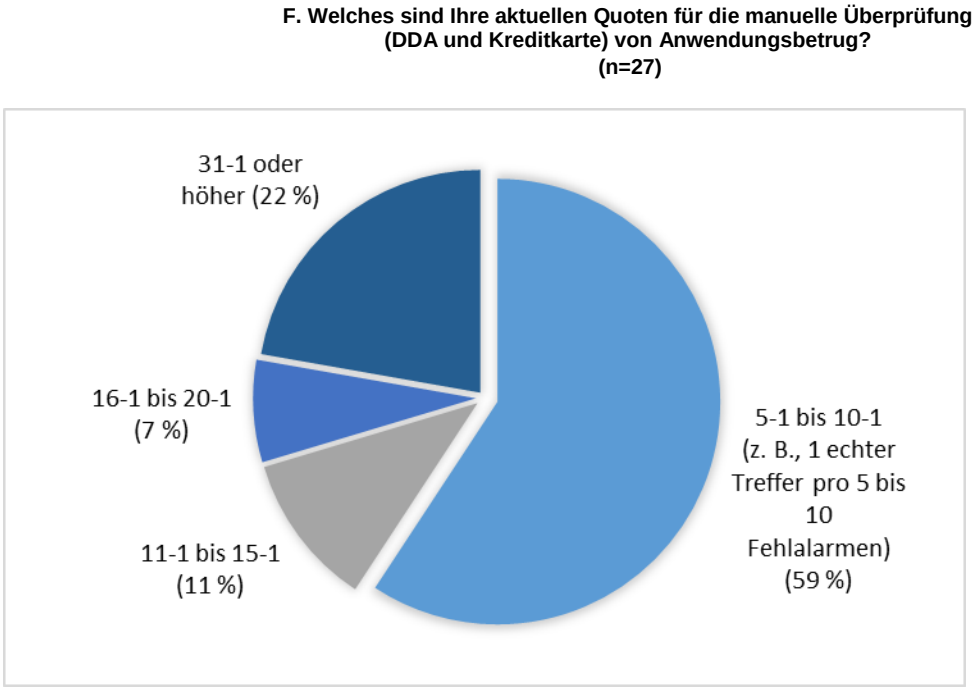
Der Identitätsabgleich ist besonders bei Datenfeldern wie Adressen problematisch. Zum Beispiel enthalten einige Adressen mehrere Wörter (die nicht immer enthalten sind), und Abkürzungen, die nicht übereinstimmen, was zu Fehlalarmen führt. Manchmal kann jeder Bewohner einer Wohnanlage aufgrund einer unscharfen Adressübereinstimmung getriggert werden, wodurch unzähligen, manuellen Überprüfungen erforderlich sind. Ein weiteres Beispiel betrifft die Namen. Ein Kunde kann ein „Junior“ sein, verwendet dieses Suffix allerdings nicht immer oder kürzt es mit „Jr.“ ab. Solche Abkürzungen können auch beim Namensabgleich problematisch sein, was zu das manuelle Review-Volumen zusätzlich steigert.

Tippfehler erhöhen nicht nur die Rate der manuellen Überprüfung, sondern sind auch teuer. In vielen Fällen erfordern die Fehler die Kontaktaufnahme mit dem Antragsteller, um sicherzustellen, dass die Daten entsprechend korrigiert werden. Anschließend müssen die korrigierten Daten erneut durch sämtliche Betrugsfilter geleitet werden. Die Wiederholung von Anfragen von Kreditbüros und anderen Betrugsfiltern führt zu zusätzlichen Gebühren von diesen Anbietern.

Mitarbeiter sind immer die größte Ausgabenposition für ein Finanzinstitut, sodass alle Prozesse, die einen erhöhten menschlichen Aufwand erfordern, kostspielig sind. Der höhere Personalbedarf zur Bewältigung vieler Falschmeldungsraten erhöht die Kosten der Betrugsprävention. Die einzige Alternative, die einige Finanzinstitute aus der Notwendigkeit heraus nutzen, besteht darin, sich für so viele Warnungen wie möglich zu entscheiden und den Rest zu löschen. Es versteht sich von selbst, dass bei diesem Ansatz betrügerische Elemente übersehen werden können, es sei denn, die Alerts verfügen über eine gute Risikopriorisierung.

Manuelle Überprüfungsraten sind bei Anwendungsbetrug aufgrund der Herausforderungen einer effektiven Identitätsprüfung tendenziell hoch. 22 % der Befragten berichten von manuellen Überprüfungsraten von 31 zu 1 oder höher (d. h., nur ein echter Treffer pro 31 oder mehr Fehlalarmen), während 41 % der Befragten von falsch positiven Werten von mehr als 11 zu 1 berichten (Abbildung 5).

Abbildung 5: Manuelle Überprüfungsraten



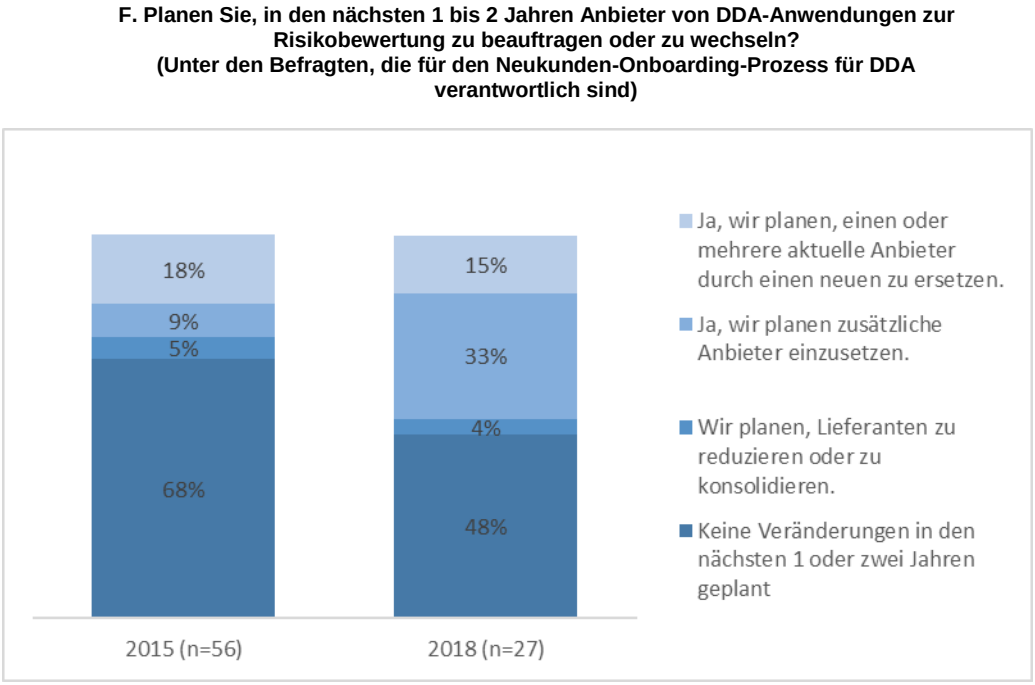
Quelle: Umfrage der Aite Group unter 30 FI, März bis Juni 2018

Diese hohen Raten der manuellen Überprüfung sind besonders problematisch, da Führungskräfte zur Bekämpfung von Finanzkriminalität unter starkem Druck von ihrem Management und Investoren stehen, die Betriebskosten (OpEx) zu senken. Die anhaltende Erwartung für die meisten der befragten Führungskräfte in Finanzinstituten besteht in einer OpEx-Senkung von 10 % oder mehr. Oder umgekehrt: Wenn Finanzinstitute durch die Reduzierung der aktuellen manuellen Überprüfungsraten effizienter werden, haben sie die Möglichkeit, bestehende Ressourcen auf neue Arten von Betrug, wie z. B. Echtzeitzahlungen, zu verlagern, ohne zusätzliches Personal aufzustellen.

DER BEDARF AN NEUEN LÖSUNGEN

Infolge des sich verschärfenden Bedrohungsumfelds und des Wettbewerbsdrucks zur Verringerung der Unstimmigkeiten plant fast die Hälfte der Befragten, in den nächsten Jahren Anbieter von Neukunden-Risikobewertungen zu wechseln oder weitere zu beauftragen. Dies entspricht einem Anstieg gegenüber 2015, als nur 27 % der Befragten beabsichtigten, Anbieter von Neukunden-Risikobewertungen zusätzlich zu beauftragen oder zu wechseln (Abbildung 6).

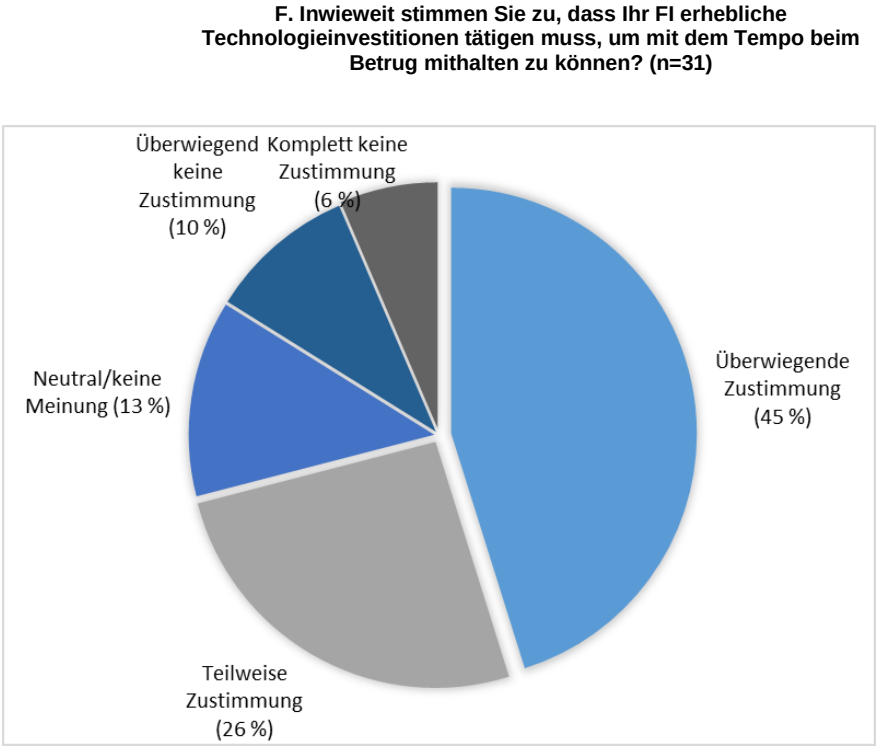
Abbildung 6: Geplante Änderungen bei Lieferanten von DDA-Anwendungen zur Risikobewertung



Quelle: Umfrage der Aite Group unter 30 FI, März bis Juni 2018, und Umfrage der Aite Group unter 83 US-FI, November bis Dezember 2015

Die Bedeutung kontinuierlicher Investitionen in neue Technologien ist nicht zu unterschätzen. 71 % der für Betrugsbekämpfung zuständigen Führungskräfte aus größeren Unternehmen glauben, dass ihr Finanzdienstleistungsunternehmen erhebliche Investitionen tätigen muss, um mit dem Tempo beim Betrug mitzuhalten (Abbildung 7).

Abbildung 7: Strategische Bedeutung von Investitionen in die Betrugsbekämpfung



Quelle: Umfrage der Aite Group unter 32 Führungskräften zur Bekämpfung von Finanzkriminalität, September 2018

Das Tempo, mit dem Betrug eskaliert und sich beschleunigt, ist nicht das einzige Problem. Eine wirksame Betrugsbekämpfung stellt für Finanzdienstleistungsunternehmen zunehmend ein Wettbewerbsproblem dar. Diejenigen, die die Technologien der nächsten Generation frühzeitig anwenden, werden in der Lage sein, mehr zu tun als nur Betrug zu reduzieren. Die damit verbundenen Verbesserungen der Customer Experience verschaffen ihnen einen entscheidenden Vorteil gegenüber ihren Wettbewerbern, die mit diesen Investitionen im Rückstand sind. Daten sind die neue Währung, und die Schaffung von optimalen Informationen aus Daten kann den Unternehmen zu einem Wettbewerbsvorsprung verhelfen.

MELISSA: WENIGER SORGEN BEI DER IDENTITÄTSPRÜFUNG

Während die Finanzinstitute nach neuen Wegen suchen, um die doppelten Herausforderungen der Verringerung der Unstimmigkeiten bei Kunden und der des Betrugsrisikos anzugehen, bietet Melissa eine Lösung. Ihre ID-Verifizierungstechnologie beinhaltet einen vielschichtigen Prozess für den Zugriff auf maßgebliche Datensätze aus Ländern auf der ganzen Welt, die Milliarden von Datensätzen enthalten, um eine Identität sofort zu überprüfen. Der Prüfprozess beinhaltet auch die nationale Identitäts- und Altersverifizierung und kennzeichnet verdächtige Personen, die auf einer von Dutzenden Überwachungslisten des Office of Foreign Assets Control und der Europäischen Union erscheinen. So können Risiken minimiert und intelligentere Entscheidungen darüber getroffen werden, was als nächstes zu tun ist: genehmigen, ablehnen oder ausweiten.

Melissas lange Geschichte der Normierung von Daten nach etablierten Standards hat zu speziellem Fachwissen geführt. Dieses erhöht die Genauigkeit der Übereinstimmung und reduziert Fehlalarme. Gleichzeitig wird sichergestellt, dass die eingehenden Daten gültig sind und die Identität des Kunden bestätigen. Wenn die Datenqualität nicht Teil der Onboarding-Lösung ist, basiert die Abgleichstechnik zwischen eingehenden Identitäten und dem Speicherort auf der einfachsten Form des exakten Abgleichs. Ohne Datenqualität können minderwertige Identitätsprüfungslösungen keine Probleme mit kritischen Feldern feststellen, wie z. B. ein fehlendes Straßensuffix, einen falsch geschriebenen Straßennamen oder einen Städtenamen (North Logan für Logan, Utah), der, wenn er standardisiert und korrigiert würde, zu genaueren Übereinstimmungen führen und das Risiko verringern würde, dass nicht vertrauenswürdige IDs durchrutschen (Abbildung 8).

Abbildung 8: Melissa gibt Match-Informationen über viele Attribute zurück

Quelle: Melissa

MOBILTELEFON-ÜBERPRÜFUNG

Die Herausforderung der Identitätsprüfung beschränkt sich nicht nur auf das Onboarding. Finanzinstitute haben auch mehrere Anwendungsfälle, die ein periodisches Bereinigen der vorhandenen Kundendaten erfordern. Ein Paradebeispiel ist der US-Personenzahlungsdienst „Zelle“ der verlangt, dass Finanzinstitute eine Handynummer für alle registrierten Benutzer hinterlegt haben. Allerdings wissen Finanzinstitute oft nicht, ob die für ihren Kunden hinterlegte Telefonnummer noch gültig ist, geschweige denn, ob es sich um eine Handynummer handelt. Melissas umfangreiche Datenbestände, kombiniert mit der Matching-Technologie, ermöglichen es einem Finanzinstitut, seinen Bestand schnell zu überprüfen, um festzustellen, welche Art von Telefonnummer für das Festnetz, Mobiltelefon oder Voice over IP registriert ist.

SCHLUSSFOLGERUNG

Finanzdienstleistungsunternehmen stehen vor der doppelten Herausforderung der sich rasch verschärfenden Finanzkriminalität und dem sich intensivierenden harten Wettbewerb um neue Kunden. Hier einige Empfehlungen für Finanzinstituts-Führungskräfte, die für die Akquisition von Neukunden verantwortlich sind:

- **Schaffen Sie eine angenehme Customer Experience für Ihre neuen Antragsteller!**
  Finanzinstitute konkurrieren nicht mehr nur miteinander, sondern auch mit Technologieunternehmen, die digitale Transaktionen für die Verbraucher so einfach und intuitiv wie möglich gestaltet haben. Suchen Sie nach Lösungen, die helfen können, Fehlalarme frühzeitig zu beheben und deren Auswirkungen auf den Kunden zu minimieren!

- **Suchen Sie nach Anbietern mit einer soliden Erfolgsgeschichte in fortgeschrittenen Matching-Routinen!**
  Verbraucherdaten sind chaotisch, aber erfahrene Anbieter in der Anwendung fortschrittlicher Matching-Algorithmen können den Unterschied zwischen einem Berg von falsch-positiven Alarmen und einer überschaubaren Anzahl ausmachen.

- **Finden Sie Lösungsanbieter mit globaler Präsenz!**
  Die zunehmende Globalisierung des Handels weitet sich auch auf das Bankwesen aus, und die Banken brauchen deshalb eine bessere Möglichkeit, neue Antragsteller zu überprüfen.

ÜBER DIE AITE GROUP

Die Aite Group ist ein globales Forschungs- und Beratungsunternehmen, das umfassende und umsetzbare Beratung zu Geschäfts-, Technologie- und Regulierungsthemen sowie deren Auswirkungen auf die Finanzdienstleistungsbranche anbietet. Mit Expertise in den Bereichen Bankwesen, Zahlungsverkehr, Versicherungen, Vermögensverwaltung und Kapitalmärkte begleitet sie Finanzinstitute, Technologieanbieter und Beratungsunternehmen weltweit. Sie arbeitet mit ihren Kunden zusammen, deckt deren Schwachpunkte auf und liefert Erkenntnisse, um das Geschäft intelligenter und stärker zu machen. Besuchen Sie die Aite Group im Web und vernetzen Sie sich auf Twitter und LinkedIn!

AUTOREN-INFORMATION

Julie Conroy
+1.617.398.5045
jconroy@aitegroup.com

Shirley Inscoe
+1.617.398.5050
sinscoe@aitegroup.com

KONTAKT

Für weitere Informationen zu Forschungs- und Beratungsleistungen wenden Sie sich bitte an:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

Für alle Presse- und Konferenzanfragen kontaktieren Sie bitte:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

Für alle anderen Anfragen wenden Sie sich bitte an:

info@aitegroup.com

ÜBER MELISSA

Melissa ist ein weltweit führendes Unternehmen für Identitäts-, Entitätsauflösung und Adressverifizierung, das Lösungen zur sofortigen Online-Verifizierung von Verbrauchern und Unternehmen anbietet. Seit 1985 verlassen sich mehr als 10.000 Kunden weltweit, darunter Finanzdienstleister, E-Commerce-Händler, Online-Gaming-Anbieter und Zahlungsanbieter, bei der Betrugsprävention sowie der Einhaltung von AML und KYC auf Melissa. Die Lösungen von Melissa bieten zur schnellen und reibungslosen Identitätsprüfung eine nahtlose Integration in bestehende Systeme.

KONTAKT

Für weitere Informationen zu den Produkten und Dienstleistungen von Melissa wenden Sie sich bitte an:

Melissa Data GmbH
Büro Europa – Standort Deutschland
Tel.: +49 (0)221 97 58 92 40
E-Mail: sales@melissa.de
www.melissa.de