Fraud Management als ganzheitliches Konzept

Von Felitas Aguilar

Silobildung ist eines der Kernprobleme im Fraud Management, meint Felitas Aguilar. Um potenzielle Betrugsfälle frühzeitig zu identifizieren, sind deshalb ganzheitliche, produkt- und kanalübergreifende Konzepte gefragt, die auch einzeln betrachtet unauffällige Vorgänge entsprechend zuordnen können. Und auch die Vernetzung der Banken untereinander gewinnt an Bedeutung. Brisant wird die Thematik vor dem Hintergrund des Konzepts „Faster Payments": Denn wenn Transaktionen innerhalb von 24 Stunden verbucht werden müssen, bleibt weniger Zeit, verdächtige Bewegungen zu entdecken. Red.

Die Urlaubszeit ist auch die Zeit, in der das Geschäft vieler Kartenbetrüger floriert. Tausende Deutsche werden sich wieder ins Ausland begeben, um zu entspannen. Doch in vielen dieser Länder, wie etwa in der Türkei oder in Südafrika, ist die Gefahr, Opfer von Kartenmissbrauch zu werden, sehr hoch. Laut BKA wurden im letzten Jahr von 619 im Ausland manipulierten Geldautomaten deutsche Daten abgegriffen, fast doppelt so viele wie noch 2007.

In Frankreich, der Türkei, Südafrika, Italien und Russland wurden dabei am häufigsten deutsche Kartendaten abgegriffen. Etwa 75 Prozent der gefälschten Debitkarten wiederum wurden laut BKA in Italien, Bulgarien, Rumänien, Großbritannien oder Frankreich eingesetzt.

Um dies zu verhindern, müssen Banken in der Betrugserkennung ein ganzheitliches und proaktives Konzept verfolgen. Sie müssen Transaktionsvorgänge in Echtzeit prüfen, damit sie den Betrug erkennen können, noch bevor er Schaden anrichtet. Auch die bessere Vernetzung der IT-Systeme innerhalb der Banken sowie der Mitarbeiter untereinander sind Schritte, die viel bewirken können.

Silos abbauen

Typischerweise sind im Laufe der Jahre entweder aus technischen Gründen oder aus Zeitmangel Vertriebskanäle nicht zusammengefügt worden. Es wurde für jeden Vertriebskanal, jedes Produkt und teilweise jede Dienstleistung ein eigenes System gebaut. Die jüngste Flut an M&A-Aktivitäten hat dazu geführt, dass die IT-Systeme der Banken gewachsen sind und nun mit verschiedenen Verzweigungen in Silos enden.

Das spiegelt sich auch darin wider, dass sich in unterschiedlichen Abteilungen unterschiedliche Teams und Systeme – unabhängig von einander – mit verschiedenen Betrugsarten befassen. Oft sind Teams, die Kartenbetrug aufdecken sollen, isoliert von Teams, die sich beispielsweise mit Online-Betrug befassen.

Hinzu kommt, dass in vielen kleineren Banken die Zuständigkeit für die Betrugsbekämpfung bei Mitarbeitern liegt, die sich nicht ausschließlich mit dem Thema Betrug befassen. Beispielsweise lastet häufig die Betrugsprävention auf den Schultern der Risikomanager. Banken sollten dafür aber Spezialisten haben, die sich ausschließlich mit dem Risiko für den Kunden befassen, damit sich Risikomanager auf das Kredit-, Investitions-, oder sonstige Risiken für Banken konzentrieren können.

Aus diesen und aus verschiedenen weiteren Gründen ist es schwierig, sich einen umfassenden Überblick über Zahlungsmuster von Kunden zu verschaffen, was für die Betrugserkennung und -prävention unbedingt notwendig wäre.

Auch für die Ermittlung von Betrügereien, die sich über verschiedene Zahlungswege erstrecken, wäre dies von Vorteil. Wenn

Zur Autorin

Felitas Aguilar ist Sales Managerin bei ACI Worldwide (EMEA), Frankfurt am Main.

beispielsweise ein Betrüger mit Hilfe von Phishing einen Angriff auf ein Konto getätigt hat, online die Adresse ändert und dann eine neue Karte bestellt, ruft das in einem silobasierten System zunächst keine große Aufmerksamkeit hervor. Denn die Teams wissen dann nicht, dass die Adressänderung gleichzeitig mit einer für den betroffenen Kunden untypischen Zahlung einhergeht, etwa wenn plötzlich eine immense Summe von einem Bankautomaten im Ausland abgehoben wird. Einzeln betrachtet, sind diese Aktivitäten nicht auffällig, in ihrer Gesamtheit aber sind sie alarmierend.

Aktuelle Techniken und Metriken zur Betrugsbekämpfung zeigen oft erst ein Problem auf, wenn die Karte bereits zwei Mal, drei Mal oder gar noch öfter für betrügerische Zahlungen verwendet wurde. Ohne einen Echtzeit-Ansatz kann die Betrugsüberwachsungslösung möglicherweise mit dem Tempo der Betrüger nicht mithalten. Je mehr Zeit vergeht, umso höher ist der Verlust und umso höher fällt der Schaden aus.

Verdächtige Transaktionsmuster über Silos hinweg erkennen

Im Hinblick auf die Risikobegrenzung ist eine Betrugserkennungslösung, die den Betrug in Echtzeit aufdeckt, entscheidend. Hierfür entwickelte Tools erlauben es den Instituten, verdächtige Transaktionsmuster über Silos hinweg zu erkennen und zu handeln, sobald der Betrüger den ersten Versuch startet, die Karte oder die Daten zu nutzen. Der Missbrauch muss also direkt gestoppt werden, bevor er entsteht. Ein regelbasiertes System analysiert alle Transaktionen bereits während des Autorisierungsprozesses. Es schlägt Alarm, sobald auffällige Transaktionen getätigt werden und verhindert deren Autorisierung.

Außerdem kann die genutzte Karte automatisch geblockt werden. Dies kann beispielsweise der Fall sein, wenn mit derselben Karte mehrere Transaktionen aus verschiedenen Ländern innerhalb kurzer Zeitspannen getätigt werden oder wenn die Abbuchung einfach nicht zu den Transaktionsgewohnheiten des Kunden passt.

Den Point of Compromise (POC) identifizieren

Mit einem ähnlichen System können Banken auch den sogenannten Point of Compromise (POC) erfassen. So können sie herausfinden, wo genau das Skimming, also das illegale Kopieren der Karte und der PIN-Nummern, stattgefunden hat. Dabei wird analysiert, wo bereits geskimmte Karten im Einsatz waren. Die Identifizierung des POC und potenziell geskimmter Karten ist wichtig, damit der Emittent Trends erkennen kann. So können die Institute in Zukunft Maßnahmen zur Aufdeckung und Verhinderung von Betrug ergreifen, bevor überhaupt ein Verlust auftritt.

Allerdings muss die Bank über eine ausreichende Anzahl an Karten verfügen, mit denen betrügerische Transaktionen getätigt wurden, um den POC festzulegen. Die Karten können wertvolle Hinweise darauf geben, wo und wann die Karten jeweils nach dem Skimming genutzt wurden, um dann Aussagen über den möglichen POC zu treffen. Sobald dies geschehen ist, können Karteninhaber identifiziert und kontaktiert werden, deren Karten poten-ziell gefährdet sind. Wenn die Bank oder das Team den Kunden nicht gleich verunsichern möchte, kann sie potenziell betroffene Konten zunächst mit Hilfe des regelbasierten Systems nur beobachten.

Proaktive Prävention verbessert Kundenbindung

Zudem besteht immer noch die Möglichkeit, die Transaktion während des Autorisierungsprozesses automatisch zu blocken. Die Parameter können individuell je nach Kundenprofil oder auf Wunsch des Kunden so eingestellt werden, dass nur dann Alarm geschlagen wird, wenn Transaktionen nicht mit den Gewohnheiten des Kunden oder den Einstellungen im System übereinstimmen. Auf diese Weise verhindert die Bank Karten- oder Kontensperrungen auf falschen Verdacht.

Die proaktive Prävention zahlt sich nicht nur im Hinblick auf die eigentlichen Betrugsfälle aus. Eine weltweite Studie von ACI Worldwide hat gezeigt, dass 49 Prozent der Befragten einen Wechsel ihres Finanzinstitutes in Erwägung ziehen würden, wenn sie Opfer eines Betruges würden oder jemanden kennen würden, der Opfer wurde und denselben Dienstleister in Anspruch nimmt.

Banken können dies verhindern, indem sie auf jeden einzelnen Betrugs- oder Verdachtsfall schnell reagieren und den Kunden telefonisch, per SMS oder per E-Mail informieren. Denn normalerweise machen Kunden ihre Bank nicht dafür verantwortlich, wenn sie zum Opfer eines Betrugs geworden sind. Doch sie machen die Bank sehr wohl dafür verantwortlich, wenn der Betrugsfall den Kunden viel Zeit und Geld gekostet hat. Mit einer gezielten Strategie, die betrügerische Transaktionen aufdeckt, noch bevor sie getätigt werden, können Banken das Kundenvertrauen und damit die Kundenbindung steigern.

Risikofaktor Faster Payments

Eine Bank, die dieses System bereits erfolgreich nutzt, ist die National Australia Bank (NAB). Sie sah sich durch die „Faster-Payments"-Kultur in Australien einem besonders hohen Gefahrenpotenzial ausgesetzt. Anders als hierzulande werden in Aus-tralien Transaktionen in der Regel innerhalb von 24 Stunden verbucht – der Bank bleibt kaum Zeit, verdächtige Be-wegungen zu entdecken und nachzuverfolgen.

Die ausgefeilte und regelbasierte Risk-Management-Lösung der NAB basiert auf dem Proactive Risk Manager von ACI Worldwide. Mit ihr werden sowohl geografische Daten als auch Daten zu spezifischen Verhaltensweisen der Kunden erhoben und im Hinblick auf Trends und Muster ausgewertet. Die Ergebnisse werden in eine Datenbank eingespeist. Wo früher lediglich statische Regeln für die Überprüfung von Transaktionen zur Verfügung standen, greift das Sicherheitssystem nun auf diese fortwährend aktualisierten Informationen zu und gleicht jede Aktion des Benutzers in Echtzeit mit seinem Profil ab. Sobald ein Vorgang nicht ins Muster passt, erhält der zuständige Bankmitarbeiter eine Warnmeldung und kann sofort reagieren.

Seit die NAB dieses System nutzt, ist der Kartenbetrug um 80 Prozent zurückgegangen. Was dort schon gang und gäbe ist, kann Modellcharakter für deutsche Banken haben. Denn im Zuge der Sepa-Richtlinie müssen künftig auch in Europa Transaktionen innerhalb von 24 Stunden verbucht werden.

Übergreifendes Enterprise Risk Management ist gefragt

Entscheidend für den Gesamterfolg im Kampf gegen Betrug und Missbrauch ist es, ein übergreifendes Enterprise Risk Management (ERM) zu etablieren. Um effizient gegen alle Angriffsversuche vorgehen zu können, müssen dabei alle relevanten Kanäle wie Kartenzahlungen, Online- und Mobilebanking miteinander vernetzt werden.

Dies setzt voraus, dass Risk-Management als ein alle Kanäle umfassendes Konzept verstanden wird und dass die technischen Voraussetzungen dafür geschaffen sind, alle Transaktionsnetze miteinander zu verzahnen. Dann stehen nicht mehr der einzelne Bezahl- oder Transaktionsvorgang, nicht mehr jeder Transaktionskanal im Mittelpunkt, sondern der Kunde mit seinen Transaktionsvorlieben und seinen üblichen Verhaltensweisen bei Bankgeschäften.

Dadurch ist die Betrachtung von Missbrauch im Kreditwesen nicht mehr nur eingeschränkt auf den Zahlungsverkehr. Auch der Versuch von Geldwäsche kann bereits im Keim erstickt werden. Auf diese Weise können Institutionen Verluste reduzieren, ihr Image bewahren und einen besseren Kundenservice bieten.