Marcus Glowasz / Renato Ndokaj

Finanzkriminalität – große Herausforderungen für die Banken-IT

Finanzskandale wie der Fall Panama Papers, aber auch das nach wie vor funktionierende Finanzierungsnetz des IS in Europa setzen hiesige Geldinstitute unter Druck. Der Kampf gegen Wirtschaftskriminalität und Terrorfinanzierung gerät infolgedessen immer stärker in den Fokus internationaler Regierungen und Behörden. Entsprechend lang ist bereits die Liste der getroffenen Gegenmaßnahmen: So hat das BMF mit dem Ausbau der sogenannten Financial Intelligence Unit (FIU), die ab Sommer 2017 aktiv werden soll, Geldwäschern den Kampf angesagt. Die EU-Kommission versucht ebenso Wirtschaftskriminellen den Geldhahn zuzudrehen. Besonderes öffentliches Interesse ging mit der Abschaffung der 500-Euro-Banknote einher, auch in Zukunft sind weitere Regelverschärfungen im Umgang mit Bargeld zu erwarten. Zur Debatte steht in etwa eine Obergrenze von Bargeldgeschäften wie auch eine Meldepflicht für hohe Bargeldgeschäfte.

Zunehmender regulatorischer Druck

Die öffentliche Debatte um das Bargeld ist indes nur die Spitze des Eisbergs. Seit Jahren schon steigen die gesetzlichen Compliance-Anforderungen an Europas Banken. Bereits als Folge der Terrorangriffe des 11. September 2001 mussten Geldinstitute strengere Transparenz- und Überprüfungsstandards für Kunden und deren Transaktionen implementieren. Auch durch die zuletzt wieder steigende terroristische Bedrohung, die Folgen der Finanzkrise für die öffentlichen Kassen sowie den damit einhergehenden politischen Drang, die Schwarzgeldquellen auszutrocknen, sehen sich Banken derzeit mit einer enormen Änderungsgeschwindigkeit in Sachen gesetzlicher Regulatorik konfrontiert.

Deren schwierigste und drängendste Herausforderung ist aktuell die vierte Richtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismus-Finanzierung (Anti-Money Laundering Directive – oder kurz AMLD4). Selbige muss bis Mitte 2017 von allen Instituten umgesetzt werden. Bereits heute lässt sich eine weitere fünfte Richtlinie absehen, welche sich besonders mit neuen, alternativen Finanzwegen befassen soll. Aktuell sind die Details bereits in der Abstimmung.

Die vierte Anti-Money Laundering Directive verpflichtet Banken, noch umfangreicher und detailgenauer über die gesamte Dauer einer Kundenbeziehung hinweg Compliance-Überprüfungen durchzuführen. Anhand einer regelmäßigen Risikobewertung aller Kunden sind im Falle von Auffälligkeiten sofort entsprechende Schritte einzuleiten. Dieser auch als „Know Your Customer" (KYC) bekannte Prozess bedeutet einen umfangreichen Mehraufwand für sämtliche Institute. Stand bislang primär die Erstüberprüfung potenzieller Neukunden im Vordergrund, gilt es nun Prozesse und Verfahren zu finden, die eine umfassende Überwachung sämtlicher Aktivitäten im Rahmen des Customer Life Cycle gewährleisten.

Bedarf an neuen Spezialisten im Bereich Compliance

Die Anpassung an die neuen Anforderungen zwingt die Institute, an zwei Stellschrauben zu drehen. Zum einen werden die Banken nicht umhinkommen, neue Spezialisten im Bereich Compliance einzustellen, um den Mehraufwand und die gestiegene Komplexität bewältigen zu können. Gleichzeitig sind Investitionen in IT-Infrastrukturen dringend erforderlich. Banken sind mit einer Vielzahl von täglichen Geschäftsbeziehungen und -transaktionen konfrontiert. Bei nicht selten siebenstelligen Transaktionszahlen versteht es sich, dass neue technologische Hilfsmittel erforderlich sind. Der hohe Investitionsbedarf birgt jedoch Schwierigkeiten: Steigende Anforderungen an Eigenkapitalquote und das Risikomanagement setzen den Banken derzeit ebenso zu wie die anhaltende Niedrigzinsphase und die Konkurrenz durch agile Fintechs, welche die Karten in der Branche neu verteilen könnten.

Zwar sind Filialschließungen und Stellenabbau längst keine Seltenheit mehr, doch wächst gleichzeitig der Bedarf an Compliance-Experten, etwa zu Prozessoptimierung und -überwachung, stetig. Die Schlagzeilen über hohe Strafzahlungen für das Nichtein-

Marcus Glowasz, Managing Principal, und Renato Ndokaj, Principal Consultant, beide Bereich Anti-Financial Crime, Capco Deutschland

Der Einsatz von künstlicher Intelligenz und Big Data bietet für die Kreditwirtschaft nicht nur neue Möglichkeiten in der Marktbearbeitung, sondern auch die regulatorischen Anforderungen an die Bekämpfung der Finanzkriminalität lassen sich damit leichter erfüllen. Während derzeit noch die vierte Richtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismus-Finanzierung zur Umsetzung bis Mitte des Jahres ansteht, verweisen die Autoren schon auf die Vorbereitung der fünften Richtlinie. Bei vielen deutschen Instituten sehen sie allerdings derzeit noch Defizite in der IT-Infrastruktur, die ein standardisiertes und effizientes Reporting, wie es im Zuge der neuen Verordnungen erforderlich ist, erschweren. Technisch versprechen sie sich von intelligenten Analyseverfahren auf Basis von Big-Data-Auswertungen eine nachhaltige Hilfestellung im Kampf der Banken gegen Kriminelle. (Red.)

halten der Vorschriften haben die Industrie alarmiert (Tabelle). Regelverstöße können im schlimmsten Fall sogar den Entzug der Banklizenz zur Folge haben, sodass die Anpassung an die Regulatorik eine besonders hohe Priorität genießt. Banken kommen nicht umhin, eine Anpassung der eigenen Prozesse und insbesondere der IT-Infrastruktur vorzunehmen.

Hervorzuheben ist jedoch, dass der Druck bei deutschen Instituten generell größer ist als bei ausländischen Banken, da die hiesigen Wettbewerber aufgrund vergleichbar hoher Fixkosten und einer schwach ausgeprägten IT-Infrastruktur im europäischen Vergleich zu den am wenigsten effizienten Banken gehören.

IT-Infrastruktur: häufig eine gefährliche Altlast

Die stark standardisierten und unflexiblen IT-Systeme vieler Banken sind ein entscheidendes Manko bei der Umsetzung neuer Geschäftsmodelle sowie der Anpassung an regulatorische Richtlinien. Die teilweise „inhouse" entwickelte Software erfordert bei neuen Anforderungen einen immensen Anpassungsaufwand, der nicht nur viel Zeit, sondern auch einen hohen Ressourceneinsatz erfordern kann. Systeme und Applikationen sind zudem in der Regel nicht für das sehr hohe Datenvolumen ausgelegt. Bestehende Systeme können teilweise nicht an neue regulatorische Anforderungen angepasst werden, da sie häufig nicht konfigurierbar sind. Das Fehlen von Standardschnittstellen zu weiteren Bankenapplikationen macht außerdem eine intelligente Verknüpfung unmöglich. Ein standardisiertes und effizientes Reporting, welches im Zuge der AML-Verordnungen erforderlich ist, lässt sich mit den wenigsten der vorhandenen Softwares umsetzen. Umso größer ist der Bedarf an smarten Lösungsansätzen abseits der bekannten Pfade.

Im Ringen mit der Regulatorik greifen immer mehr betroffene Institute auch auf externe Dienstleister zurück, entweder für die Inhouse-Implementierung der neuen AML-Regularien oder die Auslagerung der KYC-Prozesse an Drittanbieter. Für eine effiziente Inhouse-Implementierung ist eine große Erfahrung wichtig, da die Umstellung und Einsetzung der IT-Systeme sehr große Risiken bergen kann. Gerade bei solchen häufig sehr großen Projekten, die die gesamte IT-Infrastruktur der Bank betreffen können, gibt es eine Anfälligkeit für Fehler bei der Umsetzung.

Es besteht zudem auch die Möglichkeit, KYC-Prozesse an Drittanbieter auszulagern, also ein Managed-Service-Modell in Anspruch zu nehmen. Dieses Managed-Service-Modell übernimmt die Aufgabe der zentralisierten Suche, Speicherung und Bereitstellung von spezifischen Kundeninformationen aus einer Vielzahl von global verfügbaren Datenquellen.

Tabelle: Signifikante Geldstrafen aufgrund Verstößen gegen Anti-Geldwäsche-Vorgaben von UK-/US-Regulatoren

Bank	Milliarden US-Dollar	Jahr
Deutsche Bank	0,20	2017
Deutsche Bank	0,42	2017
Mega Bank	0,18	2016
Deutsche Bank	0,43	2015
Commerzbank	1,4	2015
BNP Paribas	8,9	2014
JP Morgan Chase	2,1	2014
Standard Chartered	0,3	2014
HSBC	1,9	2012
Standard Chartered	0,7	2012
ING	0,6	2012
ABN	0,5	2010

Quellen: UK-Daten: http://webarchive.nationalarchives.gov.uk/20130301170532/http://www.fsa.gov.uk/about/press/facts/fines; US-Daten: https://www.fincen.gov/news-room/enforcement-actions?field_date_release_value=2002-01-01&field_date_release_value_1=2017-02-02&field_tags_financial_institution_target_id=660

Kostensenkung durch Auslagerung

Durch das Outsourcing dieser Prozesse können Banken ihre KYC-Kosten um schätzungsweise 30 bis 40 Prozent verringern. Mit diesen Ersparnissen werben unter anderem verschiedene Dienstleister wie Thomson Reuters. Die Bank sendet dazu die zu überprüfenden Kundendaten an den Service Provider und erhält von diesem einen mit relevanten Daten angereicherten und anhand geltender KYC-Policies vollständig geprüften und analysierten Kundendatensatz zurück.

Was zunächst effizient und hilfreich klingt, stößt in der Praxis allerdings auf viel Skepsis, da noch einige Herausforderungen und Stolpersteine im Weg stehen. So existiert noch keine Standardisierung der von Drittanbietern angebotenen Services, weil Regulatoren nicht vorgeben, wie diese adäquat konzipiert sein sollten. Entsprechend kann dies zu Diskrepanzen zwischen den Anbietern und deren Resultaten führen. Für etwaige Fehler der Analyse haftet außerdem weiterhin der Auftraggeber (vergleiche MaRisk AT. 9 i.V.m. § 25 a Abs. 1 KWG). Viele betroffene Banken wollen dieses Risiko lieber vermeiden und zögern darüber hinaus auch, vertrauliche Kundendaten an externe Anbieter weiterzugeben.

IT-Innovationen: Data Analytics und künstliche Intelligenz

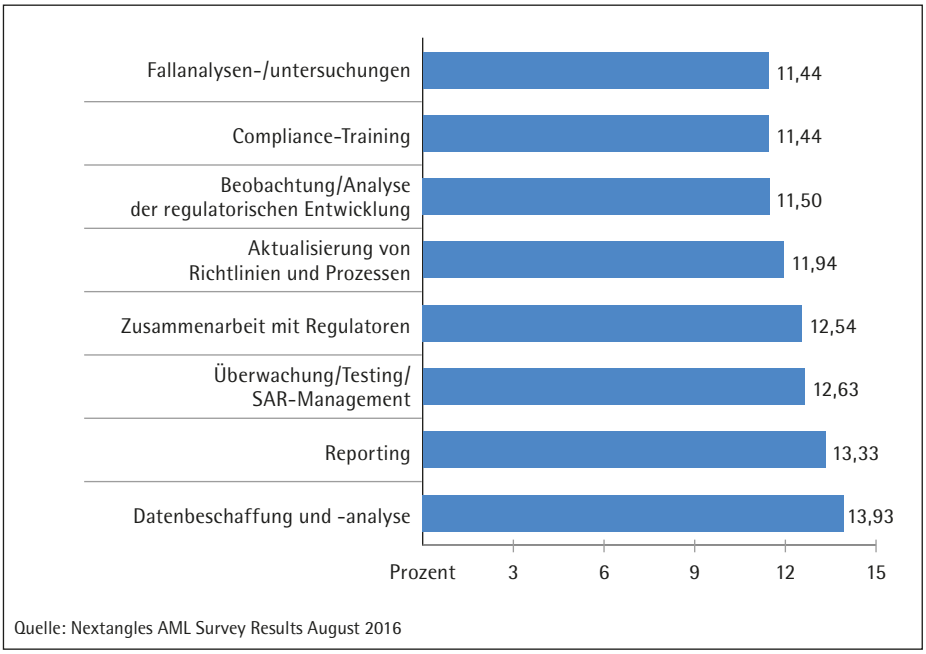
Es lässt sich feststellen, dass viele Wettbewerber weiterführende Automatisierungen durch intelligentere Systeme vornehmen. Ziel der Umstellung ist, den geltenden AML- sowie KYC-Regularien möglichst ressourcensparend und effizient zu begegnen.

Der Markt hat inzwischen einige Big-Data-Technologien (zum beispiel Apache Hadoop) hervorgebracht, mit deren Hilfe sehr große Bestände von Kunden- beziehungsweise Transaktionsdaten auf Anomalien geprüft werden können, um bestimmte Geldwäschemuster frühzeitig zu erkennen. Diese Art von automatischen Datenanalysen können die Prozesse der Compliance-Prüfungen innerhalb der Bereiche von

KYC, Transaction Monitoring, und Watchlist-Filtering wesentlich vereinfachen und gleichzeitig erheblich beschleunigen. Dabei sind die Programme so weit entwickelt, dass sämtliche Schriften und Sprachen dechiffriert und analysiert werden. Informationen in nicht lateinischen Schriftarten werden somit ebenso genutzt wie Informationen in deutscher beziehungsweise englischer Sprache.

Die zunehmenden Anforderungen zur besseren Erkennung von potenziellen Geldwäsche- beziehungsweise Finanzkriminalitätsfällen gehen auch einher mit einem erhöhten Bedarf an Daten aus verschiedenen Quellen. Relevant sind in dieser Hinsicht nicht mehr bloß Informationen aus Transaktionen und anderen Banking-Dienstleistungen: Auch ein Screening anderer Aktivitäten im Internet wird vorgenommen. So sammeln und analysieren die neu entwickelten Programme auch weitere Nutzerdaten etwa aus den Aktivitäten in den sozialen Netzwerken.

Abbildung: Durchschnittlicher Aufwandsanteil von Compliance-Tätigkeiten am Compliance-Gesamtaufwand bei Banken



Quelle: Nextangles AML Survey Results August 2016

Genaue Datenanalysen – Lösungen auch durch lernende Systeme

Im zentralisierten Datenmanagement, in dem alle für AML-Prüfungen zusammengetragenen Daten erfasst werden, können sogenannte AI-Lösungen mittels künstlicher Intelligenz genaue Datenanalysen vornehmen. So ist es beispielsweise möglich, sinngemäße Beziehungen zwischen Daten zu erkennen und diese zu interpretieren. Diese semantischen Technologien haben den Zweck, logische Relationen aufgrund semantischer Bedeutungen zwischen Daten beziehungsweise Begriffen herzustellen und darauf basierend entsprechende Schlussfolgerungen zu ziehen. Bei Auffälligkeiten der untersuchten Inhalte oder der Verknüpfungen von untersuchten Personen werden die verantwortlichen Bankmitarbeiter auf den Kunden aufmerksam gemacht, sodass weitere Prüfungen eingeleitet werden können.

Schon heute geht der Trend außerdem hin zu lernenden Systemen, bei denen die Systeme aus den vorhandenen Daten und deren Beziehungen untereinander sowie aus den getroffenen Compliance-Entscheidungen lernen. Sie sind selbstständig in der Lage, existierende AML-Regeln bei Bedarf anzupassen. So kann beispielsweise der Risikograd eines Landes durch das System erhöht werden, wenn eine bestimmte Anzahl von dubiosen Transaktionen oder Kunden erkannt worden ist. Mithilfe dieser Softwarelösungen lässt sich ein Großteil der sonst manuellen Tätigkeiten abdecken und automatisieren, insbesondere im KYC-Bereich sind die Vorteile immens. Entsprechend verringert der technologische Einsatz die Aufwände für Relationship Manager und das Compliance-Personal, da diese sich dann auf die Ergebnisse der Datenanalysen konzentrieren können, statt zusätzlich auch die Daten für eine Entscheidungsgrundlage zusammenzutragen (Abbildung).

Investitionen unumgänglich

Der Kampf gegen Terrorfinanzierung und Wirtschaftskriminelle wird Regulierer und Bankinstitute auch in den nächsten Jahren weiter beschäftigen. Es ist mit einer weiter steigenden Komplexität und noch restriktiveren Vorgaben von gesetzlicher Seite zu rechnen. Banken kommen nicht umhin, in neue und moderne Technologien zu investieren, um langfristig nicht nur kosten- und zeiteffizientere Prozesse aufweisen zu können, sondern vor allem um das Risiko von Non-Compliance zu minimieren. Bereits jetzt lasten bei einigen Instituten erhebliche Strafzahlungen auf den Bilanzen. Ein Ignorieren des technologischen und regulatorischen Trends kann für die Compliance-Verantwortlichen bei Banken unter Umständen auch persönliche Konsequenzen mit sich bringen. So sind sie für Fehler bei Due-Diligence-Aufgaben haftbar. Im schlimmsten Fall ist gar die Banklizenz gefährdet.

Fest steht, dass intelligente Analyseverfahren auf Basis von Big-Data-Auswertung Banken eine nachhaltige Hilfestellung im Kampf gegen Kriminelle bieten. Eine zeitnahe technologische Offensive macht es möglich, kriminelle Transaktionen deutlich besser aufzudecken. Gleichzeitig werden somit die Compliance-Anforderungen erfüllt, das Reputationsrisiko der Bank minimiert und mögliche Konsequenzen wie etwa Strafzahlungen ausgeschlossen.