

Anti-Financial Crime in Zeiten der Pandemie – Lessons Learned



Für Finanzinstitute stiegen durch Corona die Risiken im Bereich Geldwäsche und Terrorismusfinanzierung eminent. Compliance-Experten mussten das Tagesgeschäft teilweise radikal anpassen, um den Sorgfaltspflichten weiterhin gerecht zu werden. Welche Lehren lassen sich aus der Pandemie ziehen und wie können die neuen Erkenntnisse in Zukunft genutzt werden?

Von [Christina-Maria Pichler MA](#), [Stojan Bakalov LL.M.](#)

26. August 2021 / Erschienen in Compliance Praxis 3/2021, S. 13

Von Max Frisch ist folgendes Zitat überliefert: „Krise ist ein produktiver Zustand. Man muss ihr nur den Beigeschmack der Katastrophe nehmen“. Diese Denkweise nahmen sich in den letzten eineinhalb Jahren viele Finanzinstitute zum Vorbild, denn sie standen vor größeren Herausforderungen im Kampf gegen Geldwäsche und Terrorismusfinanzierung als je zuvor. Die COVID-19-Pandemie führte zu nie dagewesenen globalen Verwerfungen, persönlichem Umdenken und erzwungenen Strategieänderungen. Die größte Herausforderung zu Beginn der Krise war allerdings, dass die Institute zwar über Business-Continuity-Pläne verfügten und diese auch regelmäßig getestet hatten, diese Pläne jedoch das Ausmaß der Corona-Krise nicht antizipierten und daher viel zu kurz griffen. Das Motto lautete also „No Business as usual“.

Dabei ist eine sich ständig wandelnde Risikolandschaft im „Anti-Financial Crime“-Bereich keine Neuheit. Doch nur selten zuvor wurden Änderungen so schnell so drastisch spürbar wie zu Beginn der Pandemie im März 2020. Der Mangel an Vorbereitung in Kombination mit Prozessumstellungen, wie digitales Onboarding oder Telearbeit, und einem veränderten Kundenverhalten, wie vermehrtem kontaktlosem Bezahlen und Online-Banking, führten unter anderem zu KYC-Backlogs, hohen False-Positive-Resultaten im Transaktionsmonitoring und strukturell überforderten Teams.

Die Anpassung an „die neue Normalität“ brachte anfänglich viele Schwierigkeiten mit sich, doch durch das Austesten von neuen Methoden schafften die Finanzinstitute den Sprung in eine neue Welt und konnten immer wieder Erfolgserlebnisse verzeichnen. Auf ein paar der signifikantesten gewonnenen Erkenntnisse resultierend aus unseren Erfahrungen aus den vergangenen eineinhalb Jahren gehen wir im Folgenden detaillierter ein.

Regulatoren: Remote-Prüfungen statt Vor-Ort-Prüfungen

Auch wenn die Pandemie der Wirtschaft viel Luft aus den Segeln nahm, konnten Aufsichtsbehörden und Regulatoren ihre Tätigkeiten nicht einstellen. Der Versuch, Prüfungen hinauszuschieben, wurde schnell verworfen. Die Dauer der Pandemie und medienwirksame Skandale (zB FinCEN Leaks) erhöhten den Druck auf Finanzinstitute und Regulatoren enorm. Die große Frage lautete: „Wie können Finanzinstitute bei einer Prüfung agieren, wenn Mitarbeiter im Home-Office arbeiten, essenzielle Bereiche abgekapselt sind und Prozesse umgestaltet bzw. neu priorisiert werden, um den regulären Geschäftsablauf zu schützen?“ Der Weg zum Ziel war klar: Es muss digital passieren. Die Mammutaufgabe, sicher, transparent und vor allem gründlich zu prüfen, ohne physisch anwesend zu sein, brachte sowohl logistisch als auch rechtlich große Herausforderungen. Finanzinstitute mussten vorab zur Prüfung Maßnahmen setzen, um das zu ermöglichen. Dies betraf etwa folgende Themenbereiche: Datenschutz von Mitarbeitern/Kunden, nachvollziehbare Dokumentationen/sauberes Datenmanagement, Kapazitäten/Sicherheit der IT-Infrastruktur, Management der Zugriffsrechte, Kollaborations-Plattformen und Kontroll- bzw. Koordinierungsmechanismen.

Das Management von Prüfungen ist nicht zu unterschätzen und birgt in jedem eigenen Themenbereich seine Tücken und Gefahren. Es ist deshalb nicht überraschend, dass der Erfolg einer Prüfung mit der Vorbereitung steht und fällt. Die korrekte und effiziente Digitalisierung der oben genannten Bereiche erleichtert daher nicht nur den Prüfungsaufwand für die Aufsichtsbehörde, sondern reduziert auch den finanziellen und personellen Aufwand während der Prüfungsphase für die geprüfte Partei erheblich.

LESSONS LEARNED

Praxisnahe Erkenntnisse der „Remote-Prüfungen“ für beide Parteien waren definitiv die raschere/unkompliziertere Übermittlung von angeforderten Dokumenten seitens der Regulatoren, virtuelle Führungen durch die Systeme und Prozesslandschaften und die größere Flexibilität hinsichtlich der Organisation von Terminen und Konferenzen.

Geldwäsche: Trends in der Pandemie

Geldwäsche-Trends sind immer stark an die Veränderungen des Umfelds und an die Unsicherheit der Menschen während dieser Zeit gekoppelt. Die COVID-19-Pandemie war daher ein Paradebeispiel für eine starke Verhaltensänderung von Kunden, die etwa vermehrt digitale Dienstleistungen in Anspruch nahmen. Diese Situation bot der organisierten Kriminalität einen perfekten Nährboden für neue Systeme und Herangehensweisen. In den letzten eineinhalb Jahren versuchten Täter daher, die Kontrollen der Finanzinstitute mit neuen Methoden zu umgehen. Zwei der signifikantesten Trends werden im Folgenden beleuchtet:

Eine finanzielle Notlage kann leicht ausgenutzt werden. So war beispielsweise die Übernahme von Unternehmen, die die Corona-Krise nicht überstehen (würden), ein Einfallstor für Kriminelle. Deren Ziel bei der Übernahme legal wirtschaftender Unternehmen ist es, diese als Tarnung zu nutzen, um darüber illegale Gelder zu waschen. Die Änderung des UBOs (Ultimate Beneficial Owner) in Kombination mit der Veränderung des Transaktionsverhaltens kann ein Warnzeichen für solche kriminellen Machenschaften sein.

Ein weiteres Schema, das in der Pandemie verstärkt von kriminellen Organisationen genutzt wurde, ist der Missbrauch von Einzelpersonen als sogenannte „Money Mules“. So werden Personen bezeichnet, die als Finanzagenten angeworben werden, um Gelder zu waschen. Der „Job“ der Angeworbenen besteht zB darin, illegal erwirtschaftete Gelder weiterzuüberweisen – dieses Verhalten ist strafbar. Auch hier wird die

Notlage eines Menschen, der zB durch Jobverlust oder Kurzarbeit finanzielle Einbußen erleidet und Möglichkeiten alternativer Einnahmequellen sucht, ausgenutzt. Eine Möglichkeit zur Identifikation von „Money Mules“ ist es, große Veränderungen im Umsatzvolumen des Kunden zu hinterfragen.

LESSONS LEARNED

Für Finanzinstitute ist es essenziell zu prüfen, ob ihr derzeitiges internes Compliance-Rahmenwerk in der Lage ist, COVID-19-bezogene illegale Aktivitäten zu identifizieren. Gegenüber Aufsichtsbehörden muss nachvollziehbar sein, dass angemessene interne Kontrollmechanismen verfügbar sind, um das Risiko der Finanzkriminalität basierend auf den neuen Trends zu steuern.

Technologie: Innovation als höchste Priorität

Während der Pandemie passten Kriminelle ihre Praktiken an den technologischen Fortschritt an und integrierten neue Technologien in ihren Modus operandi. Geldwäschepraktiken werden daher immer ausgeklügelter, es sind bei weitem noch nicht alle bekannt. Somit gibt es viele sogenannte „Hidden Threats“, die es rasch zu identifizieren gilt. Zusätzlich häuften sich in der Pandemie Betrugsfälle und Geldwäscheverdachtsmeldungen (oft ausgelöst durch das veränderte Transaktionsverhalten) und dadurch auch der Aufwand, diese Fälle – größtenteils immer noch manuell – zu analysieren. Aber auch andere Bereiche wie KYC (Know Your Customer) sind immer noch durch einen großen manuellen Aufwand geprägt. Daher wird es in der Zeit nach der Pandemie von noch größerer Bedeutung sein, zusätzlich zu den bereits implementierten Standard-Regeln über den Tellerrand hinauszusehen, um illegale Geldflüsse identifizieren zu können (zB Mustererkennung, Netzwerke erkennen).

Der Umstieg zu neuen technologischen Strategien und Innovationen ist daher nicht nur mehr eine Option, sondern eine Notwendigkeit, um den Sorgfaltspflichten entsprechend nachzukommen. Der Einsatz von Artificial Intelligence (künstlicher Intelligenz) kann eine Möglichkeit zur Lösung vieler Schwierigkeiten sein. Der positive Effekt kann allerdings nur durch die Reduktion des manuellen Aufwands mittels Einsatzes von smarten Technologien in Kombination mit menschlicher Expertise erzielt werden.

Die Anwendungsmöglichkeiten von künstlicher Intelligenz sind sehr breit gefächert und eine zeitintensive Vorbereitung für deren Einsatz und Erfolg unumgänglich. Themen wie IT-Kompatibilität, IT-Support, Datenschutz, Qualitätskontrollen, Transparenz, Dokumentation und Lizenzmanagement müssen hierbei berücksichtigt werden. Eine gut konzipierte und durchgeführte Unterstützung der Compliance-Arbeit durch Artificial-Intelligence-Tools verspricht Qualitäts- und Effizienzsteigerungen, umfassendere Prüfungsmöglichkeiten und die Entlastung von Ressourcen.

LESSONS LEARNED

Die Beschäftigung mit und Implementierung von technologischen Innovationen ist künftig ein Muss, um Sorgfaltspflichten erfüllen zu können. Der Einsatz von künstlicher Intelligenz kann ein Weg zu mehr Effizienz und Effektivität von Prüfungen sein. Versteckte Bedrohungen durch neue Betrugsmethoden sollten schnell identifiziert und eingedämmt werden.

FAZIT

Eine Vielzahl der pandemie-bedingten Veränderungen werden uns auch in Zukunft erhalten bleiben und zur „neuen Normalität“: Remote Working, raffiniertere Geldwäschepraktiken oder der Fortschritt im Bereich der Digitalisierung. Das Leben wird sich vermehrt online abspielen, was Kriminellen viele neue Wege eröffnet, Gelder zu verschleiern und zu waschen, und damit

Compliance-Experten vor neue Herausforderungen stellt.

Andererseits haben die vergangenen eineinhalb Jahre gezeigt, dass die Pandemie ein Anstoß für Finanzinstitute war, ihre Systeme und Prozesse zur Prävention von Geldwäsche und Terrorismusfinanzierung zu verbessern. Gleichzeitig hat dies bei vielen Unternehmen auch den Weg zur Nutzung neuer Technologien im Kampf gegen die Kriminalität geebnet.

Die Pandemie hat uns allen stark verdeutlicht, dass es zwar unmöglich ist, Betrug und Geldwäsche zu eliminieren, aber dass es möglich ist, durch Lerneffekte das Ausmaß und das Risiko deutlich zu reduzieren.

Autoren



[Christina-Maria Pichler MA](#)

Christina-Maria Pichler, MA, CFE ist Managerin im Bereich Forensics bei PwC. Ihr Fokus liegt in der Aufklärung und Prävention von Wirtschaftskriminalität - forensische Sonderuntersuchungen und der ...



[Stojan Bakalov LL.M.](#)

Stojan Bakalov, LL.M. ist bei PwC Österreich in der Abteilung Forensic Services tätig. Er unterstützt Kunden mit dem Fokus auf die Bereiche Compliance, regulatorische Anforderungen im Finanzsektor ...

[HOME](#) [UNTERNEHMEN](#) [MEDIADATEN](#) [PREMIUM-MITGLIEDSCHAFT](#) [KONTAKT](#) [AGB](#) [IMPRESSUM](#) [DATENSCHUTZ](#)
[COOKIE-EINSTELLUNGEN](#)



Copyright © 2020 LexisNexis,
a division of Reed Elsevier Inc.
All rights reserved.