Typische Fraud- und Manipulationspraktiken in Kreditinstituten

Andreas Kaup/Peter Zawilla

1 Einleitung

Das Gefährdungspotenzial für Delikt-/Schadensfälle sowie Manipulationen ist in der Finanzdienstleistungsbranche – nicht zuletzt aufgrund der „Nähe zu Geld" – sehr vielfältig und umfasst nahezu alle Bereiche eines Kreditinstitutes. Demzufolge sind selbstverständlich auch die Vorgehensweisen der Täter für „sonstige strafbare Handlungen" zu Lasten von Kreditinstituten und ihren Kunden sehr vielfältig bzw. differenziert. Die Erfahrung zeigt zudem, dass dem Einfallsreichtum und der Kreativität der internen und/oder externen Täter nahezu keine Grenzen gesetzt sind.

Dieser sowie die Beiträge von Altenseuer, Becker und Neuber geben einen strukturierten und umfassenden Überblick über typische Fraud-Praktiken und Manipulationsmuster in der Finanzdienstleistungsbranche. Dennoch kann letztlich aufgrund der vorbeschriebenen Vielfältigkeit sowie der dynamischen Entwicklung lediglich ein „grober" Überblick über die Typologien und Modi Operandi gegeben werden. Die nähere Beschäftigung mit der Aufdeckung und Aufarbeitung von Delikt-/Schadensfällen veranschaulicht jeden Tag aufs Neue, dass stets mit neuen oder geänderten Facetten von Vorgehensweisen gerechnet werden muss.[1]

Die in den Beiträgen der vorgenannten Autoren dargestellten zahlreichen Fraud- und Manipulationspraktiken sind von jedem Kreditinstitut – sofern sie dort je nach Geschäftsmodell grundsätzlich auftreten können – auch im Rahmen der aufsichtsrechtlich verpflichtend zu erstellenden institutsspezifischen Gefährdungsanalyse für „sonstige strafbare Handlungen" darzustellen und zu bewerten sowie daraus ableitend entsprechende geeignete Präventionsmaßnahmen zu entwickeln und zu implementieren.[2]

Ergänzend ist darauf hinzuweisen, dass die nachfolgend dargestellten Fraud- und Manipulationspraktiken bewusst wenig konkret beschrieben sind bzw. auf eine Darstellung der jeweiligen konkreten Vorgehensweise ebenso bewusst verzichtet wurde, um (Nachahmungs-)Tätern keine Hilfestellung oder gar Inspiration für ihr kriminelles Handeln zu geben.

[1] Vgl. hierzu auch den Beitrag von Kaup/Zawilla zum professionellen Delikt- und Schadensfallmanagement sowie zu den notwendigen Voraussetzungen und der Expertise für Fraud Management in: Zawilla, P., 2012, Strategische Komponenten im Fraud Management, S. 249 f.

[2] Einzelheiten siehe BaFin-Rundschreiben 8/2005 vom 24.03.2005 „Institutsinterne Implementierung angemessener Risikomanagementsysteme zur Verhinderung der Geldwäsche, Terrorismusfinanzierung und Betrug zu Lasten der Institute gemäß §§ 25a Abs. 1 Satz 3 Nr. 6, Abs. 1 a KWG, 14 Abs. 2 Nr. 2 GwG", vgl. auch vertiefend den Beitrag von de Lamboy zur Gefährdungsanalyse für „sonstige strafbare Handlungen" sowie Jackmuth H.-W./Zawilla, P., 2011, § 25c KWG-Pflichten, S. 151 ff.

Die dargestellten Praxisfälle sind dabei in unterschiedlichen Kreditinstituten aufgetreten und resultieren aus Erfahrungswerten sowie dem regelmäßigen Austausch der beiden Autoren in anonymisierter Form mit Experten verschiedenster Kreditinstitute.

2 Darstellung der grundsätzlichen Gefährdungslage

Allein die Zahl der in diesem Fachbuch beschriebenen Einzelbeispiele für Fraud sowie der verschiedenen möglichen Tätergruppen verdeutlicht, dass nahezu alle Bereiche – und bei weitem nicht nur die kundenbezogenen – eines Kreditinstitutes für Fraud anfällig sind.

Grundsätzlich sind an erster Stelle Einheiten zu nennen, die „bargeldnah" agieren sowie die Bereiche in Kreditinstituten, die Vermögenswerte bewegen können bzw. in der Lage sind, Geld- und Zahlungsströme zu beeinflussen. Aufgrund der Erfahrungen aus der Praxis können bestimmte Bereiche eher als andere für „sonstige strafbare Handlungen" gefährdet sein. Ausgehend hiervon kann aber praktisch kein Bereich eines Kreditinstitutes als vollkommen ungefährdet angesehen werden.

Die beiden nachstehenden Abbildungen veranschaulichen, wie groß die Zutritts-Vielfalt durch externe Personen ist und wie hoch sowie vielfältig sich die allgemeine Gefährdungslage allein in einer Geschäftsstelle eines Kreditinstitutes darstellt und wogegen sich eine Bank demzufolge auch entsprechend schützen muss.

Abbildung 1: Zutritts-Vielfalt einer Bankgeschäftsstelle

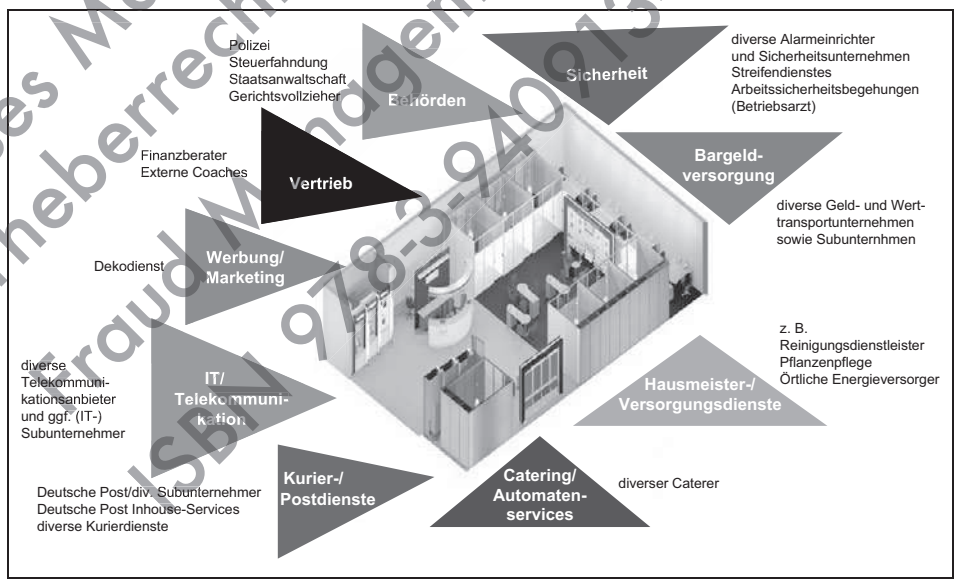
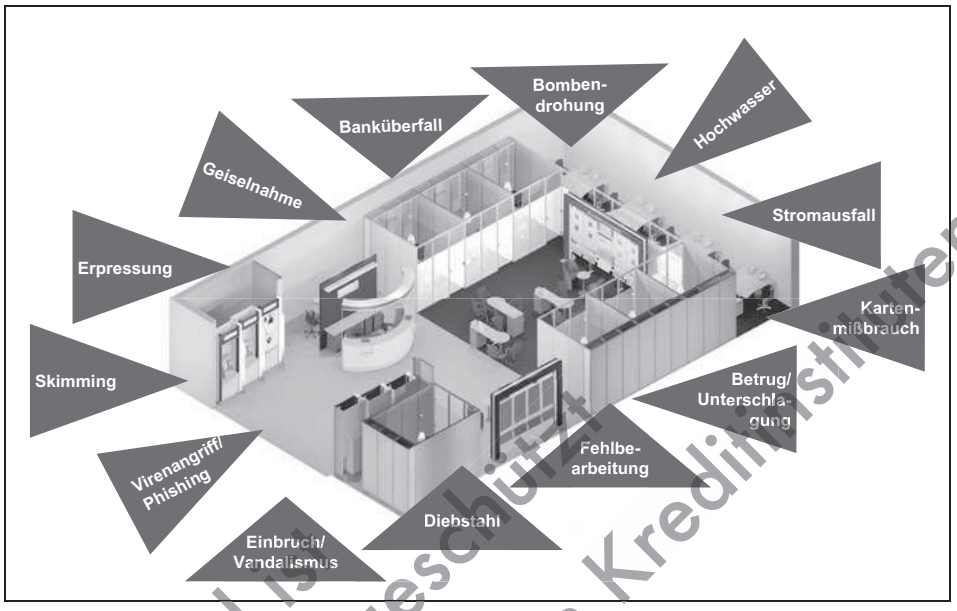


Abbildung 2: Allgemeine Gefährdungslage einer Bankgeschäftsstelle



Wie bedeutsam es ist, sich im Rahmen der Erstellung der aufsichtsrechtlich geforderten institutsspezifischen Gefährdungsanalyse für „sonstige strafbare Handlungen" auch in die Gedankengänge von Tätern hineinzuversetzen, wurde bereits im Einführungsbeitrag ausführlich geschrieben.[3]

[3] Vgl. vertiefend die Ausführungen von Jackmuth/de Lamboy/Zawilla zum ganzheitlichen Fraud Management in Kreditinstituten, zudem sind diverse Beispiele im weiteren Verlauf dieses Beitrages sowie weitere Fraud-Praktiken in den Beiträgen von Altenseuer zu Manipulationen im Vertrieb, Becker zu Fraud-Praktiken mittels moderner Zahlungsverkehrssysteme und Neuber zu Fraud-Praktiken im Bauspar- und Zuträgergeschäft beschrieben.

3 Mögliche Hinweise und Auffälligkeiten für Delikt-/ Schadensfälle sowie Manipulationen[4]

3.1 Grundsätzliche Aspekte

Wie bereits erwähnt, ist jeder Täter grundsätzlich bestrebt, so unauffällig wie möglich zu agieren, damit seine deliktischen Handlungen unentdeckt bleiben. Dabei versuchen Täter vielfach, ihre kriminellen Handlungen und Manipulationen durch weitere Manipulationen zu verschleiern.[5] Dennoch zeigt die Praxis, dass letztlich jeder Kriminelle Fehler macht, irgendwelche Auffälligkeiten verursacht oder in irgendeiner Form von sonstigen, üblichen Vorgehens-/ Verhaltensweisen abweicht. Diese Fehler, Abweichungen und Unplausibilitäten gilt es zu registrieren und zu identifizieren und anschließend natürlich weiterzuverfolgen, denn: Fehler macht jeder, man muss nur aufmerksam genug sein, diese zu erkennen! Oft sind es nur Kleinigkeiten, Kundenbeschwerden, anonyme Hinweise oder auch Zufälle, welche Täter stolpern lassen.

Bemerkenswert ist, dass nach der Aufdeckung von Unregelmäßigkeiten und Manipulationen im Rahmen der umfassenden Aufarbeitung des Falles fast immer festzustellen ist, dass es bereits zu früheren Zeitpunkten Auffälligkeiten oder Hinweise gab. Diese waren zwar Kollegen oder Vorgesetzten bekannt bzw. wurden von diesen registriert. Allerdings wurde ihnen letztlich nicht die entsprechende Bedeutung beigemessen, so dass den vorhandenen Indizien und Anhaltspunkten für deliktische Handlungen nicht weiter nachgegangen wurde und auch keine Information an die hierfür zuständigen Stellen in der Bank erfolgte (z.B. an die „Zentrale Stelle" oder die Interne Revision).

[4] Die Inhalte dieses Abschnitts sind von Zawilla auch ausführlich in dem Fachbuch von Kaup, A./Schäfer-Band, U./Zawilla, P. (Hg.), Unregelmäßigkeiten im Kreditgeschäft, 2005, S. 255 ff., beschrieben. Die Nutzung von Teilen dieser Ausführungen erfolgt mit freundlicher Genehmigung des Verlages Finanz Colloquium Heidelberg GmbH.

[5] Vgl. vertiefend die Ausführungen von Jackmuth/de Lamboy/Zawilla zum ganzheitlichen Fraud Management in Kreditinstituten, zudem sind diverse Beispiele im weiteren Verlauf dieses Beitrages beschrieben.

Manipulationen im Vertrieb

Frank Altenseuer

1 Der Vertrieb – der Vertriebswettbewerb

Das Thema Manipulationen im Vertrieb, dem dieser Beitrag gewidmet ist, unterscheidet sich von den dolosen Handlungen, die seit Jahren in Kreditinstituten begangen und aufgeklärt werden. Hier geht es nicht um den Griff in die Kasse, um das Einräumen fiktiver Kredite oder den unzulässigen Zugriff auf Vermögenswerte von Kunden oder des Kreditinstitutes.[1] Gegenstand dieses Beitrages sind vielmehr dolose Handlungen bzw. Manipulationen aus einer neuen Motivation heraus, ausgeführt mit einer neuen Qualität und zur Erreichung neuartiger Ziele.

Der Alltag in den Vertriebseinheiten der meisten Kreditinstitute hat sich, beginnend mit den Börsengängen Mitte der 1990er Jahre, gravierend verändert. Viele Häuser haben ihre Geschäfts- und Ertragspolitik verstärkt auf das provisionsträchtige (Wertpapier-)Geschäft ausgerichtet. Vor dem Hintergrund sich etablierender Direktbanken wurde die Neukundengewinnung priorisiert. Gleichzeitig wurden die Vorgaben für Absatz- und Ertragsziele immer weiter angehoben und auf den einzelnen Vertriebsmitarbeiter heruntergebrochen. Der Vertriebswettbewerb war geboren. Heute prägt er die Tätigkeit der Mitarbeiter in den Filialen stark.

Was macht diesen Wettbewerb aus? Das Kalenderjahr wird in (lückenlose) Vertriebszeiträume aufgeteilt; im Fokus jedes Zeitraums stehen ein oder mehrere Schlüsselprodukte, deren Absatz hoch priorisiert wird. Diese Schlüsselprodukte entstammen der gesamten Produktpalette, es kann sich ebenso um Neuemissionen am Aktienmarkt wie um Kredit- oder Sparprodukte, aber auch um Bauspar- oder Versicherungsprodukte von Kooperationspartnern handeln.[2] Die Messung des Vertriebserfolgs erfolgt permanent (jährlich/quartalsweise/monatlich/wöchentlich/täglich); typisch sind die jeweils hohe Priorität des aktuellen Wettbewerbs, eine i. d. R. ambitionierte Zielvorgabe sowie eine enge Begleitung durch die jeweilige Vertriebssteuerung bzw. die Führungskräfte. Die Zielerreichung ist hierbei konkret messbar und transparent. Für den Vertriebsmitarbeiter sind zwei markante wirtschaftliche Entwicklungen feststellbar: Zum einen wird die etablierte Festgehaltzahlung in immer weiterem Maße durch leistungsorientierte, variable Gehaltsanteile (Provisionen, Bonifikationen, Gratifikationen etc.) ersetzt, zum anderen wurden bei zahlreichen Kreditinstituten spezielle Veranstaltungen für die Sieger dieser Vertriebswettbewerbe ausgelobt und etabliert – sehr häufig prestigeträchtige *all-inclusive*-Veranstaltungen an Wochenenden mit attraktivem Rahmenprogramm.

[1] Vgl. hierzu ausführlich den Beitrag von Kaup/Zawilla zu typischen Fraud- und Manipulationspraktiken.

[2] Vgl. hierzu vertiefend den Beitrag von Neuber zu Fraud-Praktiken im Bauspar- und Zuträgergeschäft.

Durch den Vertriebswettbewerb wird in starkem Maße die Konkurrenzidee gefördert; das jeweilige Vertriebsranking entwickelt sich mehr und mehr zum ausschlaggebenden Karriereschlüssel für den Vertriebsmitarbeiter. Der Vertriebswettbewerb erzeugt Druck auf die beteiligten Mitarbeiter. An dieser Stelle entstehen Täter, die diesem Vertriebsdruck nachgeben – Täter, deren Handlungen bislang vielfach nicht im Fokus von Revisionsabteilungen und/oder der „Zentralen Stelle" standen. Mit diesem Beitrag soll der Blick auf die hieraus entstehenden Risiken gerichtet werden.

2 Vertriebsspezifische Manipulationsmuster

Ohne den Anspruch auf Vollzähligkeit werden in den nächsten Abschnitten fünf im Vertrieb häufig anzutreffende Felder bzw. Ansätze für Vertriebsmanipulationen vorgestellt. Die im Folgenden erläuterten Vorgehensmuster haben sich im Vertrieb in den vergangenen Jahren entwickelt und etabliert. Sie stehen beispielhaft für die jeweilige Methodik und entwickeln sich inhaltlich permanent weiter. Ausschlaggebend für den Internen Revisor, den Fraud Manager bzw. den Mitarbeiter der „Zentralen Stelle" muss hier sein, sich in das Vertriebsdenken der Kollegen hineinzuversetzen und den Blickwinkel neu zu fokussieren.[3]

2.1 Neukundengewinnung einmal anders

Ein im Vertriebswettbewerb regelmäßig hoch priorisiertes Ziel ist die Generierung von hochwertigen (Neu-)Kunden. Die Klassifizierung als hochwertig meint hier üblicherweise Mehrproduktnutzer mit uneingeschränkter Bonität und Datenqualität. Zur Erreichung dieses Ziels müssen nun die Vertriebsmitarbeiter Neukunden dieser „Güteklasse A" gewinnen, was jedoch zum einen arbeitsintensiv ist und zum anderen dadurch erschwert wird, dass diese Kunden auch Wunschkunden anderer Kreditinstitute sind und zumeist nicht als ausgeprägt wechselwillig charakterisiert werden können. Kreative Vertriebsmitarbeiter setzen bei der Tatsache an, dass ihnen lediglich quantitative Vorgaben gemacht werden und die spätere Ertragsstärke der gewonnen Kunden zunächst außer Acht bleibt. Somit können die zu liefernden Neukunden problemlos eingekauft bzw. „abgefischt" werden, sobald vielversprechende *target areas* identifiziert wurden. Das Vorgehen ähnelt tatsächlich der Schleppnetzfischerei, und die „Fischgründe" sind häufig

[3] Vgl. zu den folgenden Ausführungen Altenseuer, F./Zawilla, P., 2007, Manipulationen im Provisionsgeschäft, S. 21 ff., sowie Altenseuer, F./Zawilla, P., 2008, Manipulationen von Zielwerten im Vertrieb, S. 6 ff.

Wohnblocks mit vielen Bewohnern in eher finanzschwachen Verhältnissen, wie der folgende Praxisfall belegt:

> ***Praxisfall**: Zur Erreichung der ambitionierten und für die Bemessung der Leistungsgratifikation hoch priorisierten Zielvorgabe für die Gewinnung von Neukunden haben Außendienstmitarbeiter eines Finanzdienstleistungsunternehmens in Wohnblocks mit vielen Anwohnern in eher finanzschwachen Verhältnissen (Spar-)Geschenkgutscheine mit einem Kontoguthaben in Höhe von 5 EUR herausgegeben. Als „Gegenleistung" wurden viele der Anwohner zur Eröffnung einer Kundenverbindung bewegt, wobei allerdings von Beginn an wenig bis keine Aussichten auf eine ertragreiche, langjährige Geschäftsbeziehung bestanden.*

Wie im Praxisfall dargestellt, reicht tatsächlich zumeist die Ausgabe von so genannten Spargeschenkgutscheinen über geringe Beträge von i.d.R. 5 EUR, um aus einem Nichtkunden einen Neukunden zu machen. Die Überzeugungskraft solcher Geschenke verfehlt ihre Wirkung in der Praxis ebenso wenig auf Schulhöfen wie in Jugendclubs, Seniorenwohnanlagen, Einrichtungen für betreutes Wohnen bis hin zu Einrichtungen des Justizvollzugs. In kürzester Zeit werden hier beeindruckende Neukundenzahlen „produziert"; die ernüchternd geringen Ertragserwartungen für das Kreditinstitut bleiben hierbei unberücksichtigt. In Abhängigkeit von krimineller Kreativität und Vertriebsdruck der Mitarbeiter kommt es immer wieder auch zu Aktionen wie der kalten Akquise im wahrsten Sinne des Wortes.

> ***Praxisfall**: Ebenfalls zur Erreichung der Zielvorgabe für Neukunden haben Mitarbeiter einer Vertriebsorganisation fingierte Neukundenverbindungen eröffnet. Die entsprechenden Namen und Geburtsdaten der Kunden wurden von Grabsteinen auf einem Friedhof abgeschrieben, die dazugehörigen Wohnadressen frei erfunden und die Legitimationsdaten von bestehenden oder bereits aufgelösten Kundenbeziehungen übernommen.*

Fiktive Adressen und Legitimationsdaten sowie falsifizierte Unterschriften ergänzen die Kontoeröffnungsunterlagen.[4] Da hier vorsichtigerweise lediglich Sparkonten eingerichtet werden (die nach aller Wahrscheinlichkeit umsatzlos bleiben), wird die anfallende Korrespondenz – und damit das Entdeckungsrisiko – auf ein Minimum reduziert.

[4] Siehe hierzu auch Abschnitt 3.1.

2.2 „Veredelung" von Kunden

Eine weitere Option, die bereits erwähnten hochwertigen Kunden zu gewinnen, besteht in der „Veredelung" bereits vorhandener Bestandskunden, die bis dahin jedoch faktisch lediglich Kunden mit eingeschränkter Bonität waren. Dies wird üblicherweise durch die IT-technische Löschung von kritischen Merkmalen wie negativen Bonitätskennzeichen oder fehlenden Legitimationsdaten erreicht.

Ein alternativer Ansatz ist die Generierung fiktiver Kunden. Hiermit ist nicht nur das langjährig bekannte Produzieren nicht existenter natürlicher Personen in den Datenbestand von Kreditinstituten zu verstehen (zu deren Erkennung i.d.R. Prüfroutinen implementiert sind), sondern immer häufiger auch der Import von Bestandskunden von Kooperationspartnern in den eigenen Bestand, ohne dass diese Kunden von ihrer neuen Bankkontoverbindung wissen. Die immer engere Zusammenarbeit von Vertriebsmitarbeitern mit Mitarbeitern von Versicherungsagenturen, Bausparkassen o.ä. erleichtert hier auch eine illegitime und nicht legale Kooperation.

Der Vollständigkeit halber sei hier auch die Unterdrückung von Kundenabgängen genannt. Die Entwicklung der Kundenanzahl ist als Verrechnung der Neukunden gegen die Kundenabgänge zu bewerten, wobei immer wieder Vertriebserfolge im Wesentlichen dadurch erzielt werden, dass abschließende Kontoauflösungen unterbleiben. Beispielhaft seien hier die in den meisten Kreditinstituten periodisch vorgenommenen Ausbuchungen unbewegter Kleinstsparkonten genannt; in der Konsequenz kann dieser Ansatz jedoch sogar soweit führen, dass Kontoinhabern, denen eine nicht legale Nutzung ihres Kontos nachgewiesen wurde, die Geschäftsbeziehung nicht mehr gekündigt wird, um die Kundenanzahl nicht zu reduzieren.

2.3 Reduzierung von Zielvorgaben

Üblicherweise werden in jedem periodischen Vertriebswettbewerb transparente Kennziffern zur Erfolgsmessung vorgegeben. Sehr häufig findet hierbei in Kreditinstituten eine Ertragsgröße wie etwa der Wertpapierhandelsertrag Verwendung. Dieser wird typischerweise als prozentuale Vorgabe im Bezug auf ein bestehendes Depotvolumen vorgegeben. Die Festlegung erfolgt mittels mathematischer Verfahren; hierzu wird auf Bestandsgrößen (wie bspw. das betreute Depotvolumen) zugegriffen. Üblicherweise findet hierbei jedoch nicht das Bruttogesamtvolumen Berücksichtigung. Sinnvollerweise werden hier solche Depotvolumina, die etwa als Kreditsicherheit dienen, herausgerechnet.

Die genaue Kenntnis dieser Parameter sowie des Stichtages für die Zielwertbestimmung ermöglicht es dabei Vertriebsmitarbeitern, in den Banksystemen einen signifikanten Teil des von ihnen verwalteten Depotvolumens für einen kurzen Zeitraum manipulativ als

Professionelle Trader in einer Gefangenendilemma-Situation

Thomas Noll/Pascal Scherrer

1 Ausgangslage

Die immensen Verwerfungen an den Finanzmärkten ab Frühling 2007 – mit dem Untergang der US-Investmentbank Lehman Brothers im September 2008 als Höhepunkt – haben dem Ruf der globalen Finanzdienstleistungsindustrie beträchtlichen Schaden zugefügt. Unter den Banken selber war und bleibt schwindendes Vertrauen ein wichtiges Thema, weil darunter mehr als nur die Liquiditätsversorgung leidet.[1] Nachhaltige Vertrauensverluste haben die Banken nicht nur untereinander zu beklagen. Auch in weiten Teilen der Bevölkerung ist der Verlust der Glaubwürdigkeit von Banken und Finanzinstituten groß. „Die Erfahrung, dass es sowohl zu Staats- als auch zu Marktversagen kommen kann, hat die Menschen verunsichert, auf wen und was sie sich überhaupt noch verlassen können."[2]

1.1 Unternehmen in Reputationsnöten

Mit derselben Intensität, wie die Glaubwürdigkeit bei vielen großen Unternehmen in der Finanzdienstleistungsindustrie erodierte, schien die Bereitschaft der Bevölkerung abzunehmen, private Unternehmen durch öffentliche Gelder zu retten. Im Juni 2009 sprachen sich in einer repräsentativen Umfrage des deutschen Nachrichtenmagazins „Stern" mehr als 60% der Befragten gegen jede Form von staatlicher Hilfe für den schlingernden Handels- und Touristikkonzern Arcandor aus. Nur gerade ein knappes Drittel (32%) wollte dem angeschlagenen Konzern durch den Staat unter die Arme greifen lassen.[3] Ferner entfachten die erwähnten Rettungsaktionen die Diskussion um privatisierte Gewinne und sozialisierte Verluste neu. In unzähligen Internetforen und Blogs debattierten Interessierte in den Folgemonaten über die Finanzkrise – oft unter polemischen Titeln wie „Kapitalismus für die Armen und Sozialismus für die Reichen".[4]

Währenddem in den USA Fannie Mae und Freddie Mac faktisch verstaatlicht wurden, musste in der Schweiz die UBS schmerzlich erfahren, dass veröffentlichte Meinung (Medien) und öffentliche Meinung (Kunden) deckungsgleich waren. Die NZZ stellte im August 2008 auf ihrer Website einen kausalen Zusammenhang zwischen dem Reputa-

[1] Triebe, B., 2010, Wenn Banken Beziehungsprobleme haben.

[2] Bude, H., 2010, Zwischen Krisenangst und Zuversicht.

[3] Stern, 2009, Deutsche gegen Staatshilfe für Arcandor.

[4] Vgl.: http://blog.rainbownet.ch/politik-schweiz/svp/finanzkrise-und-ubs-boni, http://www.brainr.de/brainstorming/show/8048-schlagwoerter-zur-finanzkrise, http://elisabethkerschbaum.wordpress.com/2008/10/07/gewinne-privatisieren-verluste-verstaatlichen/, http://www.nzz.ch/finanzen/nachrichten/imageschaden_schlaegt_vor_allem_in_schweiz_durch_1.804887.html.

tionsproblem der Großbank und den massiven Abflüssen von Kundengeldern her: „Imageschaden der UBS schlägt stark durch“.[5] Im dritten Quartal verstärkte sich der Geldabfluss weiter, so dass die UBS-Kunden in den ersten neun Monaten des Jahres 2008 insgesamt 140 Mrd. CFH abgezogen hatten. Dies entsprach einem damaligen Anteil von mehr als 5% am UBS-Totalbetrag von 2.640 Mrd. CFH an Assets under Management.[6]

1.2 Suche nach den Schuldigen

Die Finanzmarktkrise und ihre weitreichenden Folgen brachten neben den Unternehmen auch die Akteure in der Finanzdienstleistungsindustrie in Reputationsnöte: Trader, Investmentbanker, Entwickler von hochkomplexen Finanzinstrumenten und Risikospezialisten sahen und sehen sich starker Kritik ausgesetzt. Mitunter eine Rolle spielen dabei Millionen-Boni, die, im Sinne eines Stellvertreterkrieges, in der Öffentlichkeit diskutiert und kritisiert werden. So wie im Februar 2009, als die deutsche Bundeskanzlerin Angela Merkel gegenüber dem Nachrichtenmagazin „Der Spiegel“ erklärte: „Es ist unverständlich, dass Banken, denen der Staat unter die Arme greift, in vielen Fällen gleichzeitig riesige Bonussummen auszahlen“.[7] Wenige Monate später, am 10.12.2009, bezeichnete die Kanzlerin eine Spezialsteuer auf Banker-Boni an einer Pressekonferenz als charmante Idee.[8]

Nichts zur Verbesserung der Reputation von Börsenhändlern beigetragen haben dürften der ehemalige Société-Générale-Trader Jérôme Kerviel und der UBS-Trader Kweku Adoboli. Die Händler haben ihre jeweiligen Arbeitgeberinnen durch Spekulationsgeschäfte und betrügerische Machenschaften um fast 5 (Kerviel) respektive 2 (Adoboli) Mrd. EUR geschädigt. In seinem Buch mit dem Titel *L’engrenage – mémoires d’un trader*, mit dem er sich vor seinem Prozess im Herbst 2010 als Opfer eines pervertierten Systems darstellte, setzt Kerviel seinen Egoismus mit dem angeblichen Leitgedanken seiner Zunft gleich: „Das einzige Leitmotiv ist, so viel Geld wie möglich in so kurzer Zeit wie möglich zu verdienen – egal wie.“ Seine Vorgesetzten hätten ihn, so Kerviel weiter, lange Zeit jeden Abend für seine Gewinne gelobt. „Innerhalb dieser großen Bankenorgie haben die Trader lediglich das Anrecht auf das gleiche Ansehen wie eine einfache Prostituierte: Die schnelle Wertschätzung, dass der Tag gut gelaufen ist“, urteilt er.[9]

[5] Baches, Z., 2008, Imageschaden der UBS schlägt stark durch.
[6] Schweizerische Depeschenagentur SDA, Meldung vom 4. November 2008.
[7] Merkel, A., 2009, Schuld und Sühne.
[8] Merkel, A., 2009, Kongress Europäische Volkspartei EVP.
[9] Kerviel, J., 2010, L’engrenage.

1.3 Trader im Fokus

Angesichts der geschilderten Ereignisse erstaunt es nicht, dass Trader als egoistisch, gierig, übertrieben selbstsicher und wenig risikobewusst beschrieben werden.[10] Vor dem Hintergrund der Finanzmarktkrise seien die persönlichen Verhaltensweisen von Tradern gar stärker verurteilenswert als das System im Allgemeinen oder spezielle Instrumente im Besonderen.[11] Der damit zusammenhängende und angeblich egoistische Individualismus basiert auf der Auffassung, dass *„there is no moral duty to sacrifice individual advantage for any greater good, because there simply is no greater good than personal happiness."* Marktteilnehmer verfolgen ihre jeweiligen individuellen Vorteile *„regardless of others, because individual happiness is the ultimate good"*.[12]

In dieselbe Richtung zielen Forschungsresultate, die den Schluss zulassen, dass Fairness-Überlegungen und die Kooperationsbereitschaft bei Tradern *per se* eher unwichtig sind, aber dass auf der andern Seite dem Egoismus eine übergeordnete Bedeutung zukommt. In Marktexperimenten mit kompetitivem Hintergrund, in denen klar definierte homogene Güter gehandelt werden, verhalten sich fast alle teilnehmenden Subjekte so, als wären sie einzig und allein an ihrem individuellen materiellen Erfolg interessiert.[13]

1.4 Von Selbstvertrauen, Gier und Egoismus

Um das Handeln und die Verantwortlichkeit von Tradern in der Finanzmarktkrise zu verstehen, kann auf deren Persönlichkeitsdisposition zurückgegriffen werden. In diesem Zusammenhang kommt dem Begriff des übermässigen Selbstvertrauens eine wichtige Rolle zu. Trader mit übermässigem Selbstvertrauen neigen dazu, die Exaktheit ihrer Marktinformationen zu überschätzen. Dies verleitet sie am Markt, wo die Asymmetrie von Informationen bekanntlich eine bedeutende Rolle spielt, zu falschen Beurteilungen über den Wert von Assets zu kommen. Diese falschen Beurteilungen wiederum führen zu einer starken Gefährdung der Trader, dem Phänomen des *winner's curse* zu erliegen –

[10] Lo, A./Repin, D./Steenbarger, B., 2005, Fear and greed in financial markets; Carr, E., 2009, Greed and fear; Barber, B./Odean, T. 1999, The courage of misguided conviction; Daniel, K./Hirschleifer, D./Subrahmanyam, A., 2001, Overconfidence, arbitrage and equilibrium asset pricing; Daniel, K./Hirschleifer, D./Subrahmanyam, A., 1998, Investor psychology and security market; Levy, M., 2010, Fortunately for us, a new generation is rising.

[11] Mortreuil, L., 2010, The current crisis.

[12] Belousek, D., 2010, Greenspan's folly.

[13] Smith, V./Williams, A., 1990, The boundaries of competitive price theory; Roth, A. et al., 1991, Bargaining and market behaviour; Kachelmeier, S./Shehata, M., 1992, Culture and competition; Güth, W./Marchand, N./Rulliere, J., 1997, On the Reliability of Reciprocal Fairness.

also dem Fluch des Gewinners.[14] Der Begriff des *winner's curse* entstammt der Auktionstheorie und behandelt – einfach formuliert – das Dilemma, dass Bieter eine Auktion nur deshalb gewinnen, weil sie den wahren unbekannten Wert des Versteigerungsgegenstandes von allen Mitbietern am meisten überschätzt haben. Oder anders formuliert: Je höher die Anzahl der Bietenden und je größer der Grad der Unsicherheit ist, desto intensiver bieten die Beteiligten mit. Damit einhergehend steigen nach Auktionsende die Frustration der leerausgegangenen Verlierer und das ungute Gefühl des Gewinners, möglicherweise zuviel bezahlt zu haben.[15]

Übermäßiges Selbstvertrauen äußert sich bei Tradern nicht nur, wie oben beschrieben, in der Überschätzung des Wertes ihrer Marktinformationen. Es findet seinen Niederschlag auch in den Trading-Volumina. Je überzeugter ein Händler von sich und seinen Fähigkeiten ist, desto grösser ist die Anzahl seiner Transaktionen. Nur: Die Mischung aus einem übertriebenen Selbstvertrauen, dem damit einhergehenden hohen Handelsvolumen und der Neigung, Erfolge sich selbst zuzuschreiben, steht den in der Vergangenheit erzielten Erträgen diametral entgegen.[16] Einen negativen Einfluss hat das übermäßige Selbstvertrauen von Tradern ferner bei der Prognose ihrer zukünftigen Ergebnisse. Eine über mehrere Jahre angelegte Studie mit monatlichen Vergleichen – in der die von Tradern vorausgesagte eigene Performance mit der tatsächlich erbrachten Leistung verglichen wurde – kommt zu einem ernüchternden Schluss: Die Trader-Prognosen sind unbrauchbar, weil sie in keinem Zusammenhang mit den erbrachten Leistungen stehen. Dafür offenbart die Studie bei den Tradern ein signifikant erhöhtes Mass an Selbstüberschätzung.[17]

Tief in die Psyche von Tradern schaut Kimberly D. Krawiec in ihrer Studie über Rogue Traders aus dem Jahr 2000. Sie bezeichnet die Handelsräume von Banken als Superstar-Umgebung und verweist auf die enorme Statusgläubigkeit von Tradern, die einen hohen intrinsischen Wert habe. Gier, das Eingehen von Risiken und Unabhängigkeit bildeten die drei hervorstechendsten Merkmale des institutionell-normativen Rahmens der Branche, wobei Gier nicht negativ konnotiert sei. Aufgrund der weitgehend fehlenden Aufstiegsmöglichkeiten definiere sich die Hierarchie im hochkompetitiven Geschäft nur über zwei Arten von Tradern: Jene, die für ihr Unternehmen mehr Geld verdienen und jene, die weniger verdienten. Statt wie in anderen Branchen für gute Leistungen mit beeindruckenden Titeln oder größerer Verantwortung belohnt zu werden, werde der Erfolg von Tradern mit höheren Boni abgegolten. In diesem Sinne sei Geld bei Tradern

[14] Biais, B. et al., 2005, Judgemental Overconfi-dence, Self-Monitoring, and Trading Performance.

[15] Thaler, R., 1988, Anomalies – The Winner's Curse.

[16] Statman, M./Thorley, S./Vorkink, K., 2006, Investor Overconfidence and Trading Volume.

[17] Gloede, O./Menkhoff, L., 2009, Financial professionals' overconfidence.

Gefährdungsanalyse für „sonstige strafbare Handlungen"

Christian de Lamboy

1 Einleitung

In deutschen Kreditinstituten wird täglich mit mehreren Milliarden Euro gearbeitet. Kredite werden bewilligt, Aktien gekauft oder Unternehmen auf bevorstehende Börsengänge vorbereitet. Funktioniert alles reibungslos, tritt das Thema Risiko schnell in den Hintergrund. Speziell das Risiko der Wirtschaftskriminalität wird von den Instituten häufig unterschätzt, wie Studien belegen.[1] Dabei entstehen sowohl monetäre Schäden als auch immaterielle Schäden, wie Reputations- und Vertrauensverluste.[2] Je nachdem, welcher Art ein Fall ist und ob er öffentlich bekannt wird, wirken sich wirtschaftskriminelle Handlungen zusätzlich negativ auf die Geschäftsbeziehungen zwischen Kunde und Institut aus.[3] Daher ist es elementar für Kreditinstitute, ein umfassendes Überwachungssystem zu implementieren, um kriminellen Handlungen zu Lasten des Institutes vorbeugen zu können.

Bereits Anfang 2002 wurde der Grundstein für die Eindämmung und Verhinderung wirtschaftskrimineller Handlungen in deutschen Kreditinstituten gelegt. Das Kreditwesengesetz (KWG) verpflichtet seit diesem Zeitpunkt alle Institute dazu, angemessene Sicherungssysteme zur Verhinderung betrügerischer Handlungen zu Lasten der Institute zu schaffen und zu unterhalten.[4] Seit März 2005 besteht mit der Veröffentlichung des Rundschreibens 8/2005 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die konkrete aufsichtsrechtliche Pflicht zur Erstellung einer institutsspezifischen Gefährdungsanalyse für wirtschaftskriminelles Handeln.[5] In 2008 wurde mit der Einführung des § 25c KWG die gesetzliche Grundlage für die Gefährdungsanalyse gelegt, die in den Auslegungs- und Anwendungshinweisen dargestellt wird.[6]

Der Begriff Gefährdungsanalyse beschreibt die methodische Erfassung und Identifizierung von Risiken. „Im speziellen [wird] das Risiko eines Missbrauchs von Finanzdienstleistungen zum Zwecke der Geldwäsche oder anderer Formen von Schwerstkriminalität“[7] analysiert, die in einem Kreditinstitut vorherrschen können. Bei dieser Analyse der

[1] Vgl. Bundesministerium des Inneren, 2011, Wirtschaftskriminalität; KPMG, 2013, Wirtschaftskriminalität.

[2] Vgl. Manager Magazin, 2008, Kerviel setzte 50 Milliarden Euro ein; Süddeutsche Zeitung, 2007, Der Flowtex-Fall.

[3] Vgl. Salvenmoser, S./Kruse, H., 2006, Der Täter aus den eigenen Reihen, S. 48.

[4] Vgl. Achtelik, O., 2005, Leitfaden zur Erstellung der Gefährdungsanalyse.

[5] Vgl. Jackmuth, H.-W./Zawilla, P., 2012, Erstellung einer Gefährdungsanalyse, S. 286 f.

[6] Zuletzt in Deutsche Kreditwirtschaft, 2011, Auslegungs- und Anwendungshinweise der DK.

[7] Herzog, H./Höche, T., 2009a, Neue Wege der Geldwäscheprävention, S. 56.

Gefährdungssituation gilt es, potenzielle Risiken strukturiert aufzunehmen, um im Anschluss geeignete Sicherungsmaßnahmen erarbeiten zu können.[8] Die Gefährdungsanalyse erfolgt i.d.R. durch eine detaillierte Untersuchung der Aufbau- und Ablauforganisation eines Institutes sowie aller Prozesse und Organisationseinheiten hinsichtlich des Gefährdungspotenzials.

Der vorliegende Beitrag soll eine allgemeine Einführung und gezielte Umsetzungshinweise zur Gefährdungsanalyse für „sonstige strafbare Handlungen" nach § 25c KWG geben. Die aufsichtsrechtlichen Grundlagen und Rahmenbedingungen der Gefährdungsanalyse werden nicht im Detail behandelt, da diese bereits durch den Beitrag von Ackmann in diesem Buch abgedeckt wurden.[9]

2 Grundsätzliches zur Gefährdungsanalyse

2.1 Nutzen und Notwendigkeit der Gefährdungsanalyse

Das Ziel einer Gefährdungsanalyse liegt in der Erfassung, Identifizierung und Klassifizierung der institutsspezifischen Risiken von „sonstigen strafbaren Handlungen" und Fraud zu Lasten eines Institutes oder einer Institutsgruppe, um die Institute vor diesen Handlungen zu schützen.[10] Die Bekämpfung der Wirtschaftskriminalität ist demnach Bestandteil eines wirksamen Risikomanagements und unabdingbar für die Institute.[11] Nur wenn ein Institut sich der größten potenziellen Risiken bewusst ist, kann es entsprechend wirksame Präventionsmaßnahmen zum Schutz erarbeiten.

Ohne eine tiefgreifende Untersuchung und die Aufdeckung aller Schwachstellen besteht dabei die Gefahr, dass die vorherrschenden Risiken nicht oder nur teilweise bekannt sind und somit unterschätzt werden. Logische Konsequenz dieser Schwachstellen ist, dass kein dem tatsächlich existierenden Risiko angemessenes Schutzsystem implementiert ist. Die Notwendigkeit einer Gefährdungsanalyse besteht also auch über die aufsichtsrechtliche Verpflichtung hinaus, da mit ihrer Hilfe die unternehmensspezifischen Gefährdungspotenziale erkannt werden.[12] Dies dient sowohl dem Schutz des Institutes als auch

[8] Vgl. Lindner, B./Glebovskiy, A., 2009, Betrügerischen Handlungen vorbeugen.

[9] Vgl. auch den Beitrag von Ackmann zu den regulatorischen Grundlagen bei der Bekämpfung „sonstiger strafbarer Handlungen".

[10] Ganguli, I. et al., 2010, Prävention und Bekämpfung von betrügerischen Handlungen, S. 17 f.

[11] Vgl. Jackmuth, H.-W./Zawilla, P., 2012, Erstellung einer Gefährdungsanalyse, S. 285.

[12] Vgl. Jackmuth, H.-W./Zawilla, P., 2012, Erstellung einer Gefährdungsanalyse, S. 285.

dem Schutz des Verbrauchers. Die hohen auftretenden Schadenssummen der Wirtschaftskriminalität machen deutlich, wie wichtig es ist, die Bekämpfung von Straftaten mit höchster Priorität voranzutreiben.[13]

Die verschiedenen Dienstleistungen und Schwerpunkte, welche in den jeweiligen Instituten angeboten werden, bedingen, dass es keine übergreifende Einheitslösung für das gesamte Finanzgewerbe geben kann. Dies bedeutet auch, dass jede Gefährdungsanalyse die spezifischen Gegebenheiten des Institutes individuell abbilden muss.[14] Bei der Erarbeitung kann und sollte allerdings, zwecks Erfahrungsaustauschs, mit anderen Kreditinstituten, den Bankverbänden oder externen Beratern zusammengearbeitet werden.

Auch sollten Experten aus unterschiedlichen Bereichen des Institutes mit in die Erstellung der Gefährdungsanalyse eingebunden werden. Dies sind z. B. Vertreter der Organisationseinheiten Compliance, Datenschutz, Interne Revision oder Sicherheit.[15] Aus den genannten Bereichen kann ein großes Fachwissen bezüglich bestehender und potenzieller Gefährdungsmöglichkeiten erwartet werden. Bei der Internen Revision ist jedoch darauf zu achten, dass eine direkte Projektbeteiligung aufgrund der zu wahrenden Neutralität nicht erfolgt.[16]

2.2 Zuständigkeit und Adressaten

Die Zuständigkeit für die Erstellung der Gefährdungsanalyse liegt nach § 25c Abs. 1 S. 1 i. V. m. Abs. 9 S. 1 KWG bei der für die Verhinderung der Geldwäsche, Terrorismusfinanzierung sowie der sonstigen strafbaren Handlungen einzurichtenden „Zentralen Stelle". Die „Zentrale Stelle" ist für eine Reihe von Aufgaben verantwortlich, die in Bezug auf die „sonstigen strafbaren Handlungen" zu leisten sind.[17] U.a. muss von ihr eine Definition und ständige Aktualisierung der internen Grundsätze für Zuständigkeiten, Pflichten, Verantwortlichkeiten und Prozesse innerhalb des Institutes entwickelt und geführt werden. Weiterhin sollte eine fortlaufende Aktualisierung geeigneter Strategien zur Verhinderung des Missbrauchs von neuen Produkten und Technologien sichergestellt werden, welche die Anonymität von Geschäftsbeziehungen und Transaktionen begünstigen können. Eine der Hauptaufgaben der „Zentralen Stelle" ist jedoch die Schaffung und Weiterentwicklung einer risikoadäquaten, institutsspezifischen integrierten

[13] Vgl. Bundesministerium des Inneren, 2011, Wirtschaftskriminalität.

[14] Vgl. Jackmuth, H.-W./Zawilla, P., 2012, Erstellung einer Gefährdungsanalyse, S. 290.

[15] Vgl. Jackmuth, H.-W./Zawilla, P., 2012, Erstellung einer Gefährdungsanalyse, S. 290.

[16] Vgl. Helfer, M., 2012, Fraud Management aus dem Blickwinkel der Internen Revision, S. 405-423.

[17] Vgl. Deutsche Kreditwirtschaft, 2011, Auslegungs- und Anwendungshinweise der DK.

Professionelles Delikt- und Schadensfallmanagement[1]

Andreas Kaup/Peter Zawilla

[1] Ein ähnlich gestalteter Beitrag von Zawilla befindet sich auch in: Jackmuth, H.-W./de Lamboy, C./Zawilla, P. (Hg.), Fraud Management – Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität (siehe auch entsprechenden Hinweis am Ende dieses Buches). Die grundsätzliche Vorgehensweise im Rahmen des Delikt-/Schadensfallmanagements ist branchenübergreifend zwar vergleichbar, dennoch gibt es bankspezifische Besonderheiten.

1 Notwendigkeit eines strukturierten Vorgehens

Die professionelle Bearbeitung von aufgetretenen bzw. bekannt gewordenen Fraud-Fällen, begangen durch eigene Mitarbeiter eines Kreditinstitutes und/oder Externe, bildet neben der Fraud-Prävention sowie der Fraud-Aufdeckung die dritte wesentliche Säule eines ganzheitlichen, integrierten Fraud Managements nach dem PDCA-Modell (Plan, Do, Check, Act).[2]

Materielle Verluste aufgrund von Schadensfällen durch wirtschaftskriminelles Handeln, Missmanagement oder Bearbeitungsfehler können im Einzelfall ein Ausmaß erreichen, das für ein Unternehmen eine ernsthafte Bedrohung darstellen kann. Neben den unmittelbaren wirtschaftlichen Auswirkungen erleiden die geschädigten Unternehmen zudem – aufgrund der meist unvermeidlichen Publizität dieser Vorkommnisse – oftmals einen massiven Vertrauensverlust und eine deutliche Beeinträchtigung ihrer Reputation.

Schadensfälle sollten daher jeweils als Krisenfall verstanden und entsprechend professionell behandelt werden. Ausgehend hiervon sollten Delikt- und Schadensfälle damit grundsätzlich in das Notfall- und Krisenmanagement eines Unternehmens aufgenommen werden.[3] Elementarer Bestandteil eines professionellen und dokumentierten Krisenmanagementkonzeptes sollte entsprechend ein Schadensfallmanagementleitfaden sein, der Regelungen zur Vorgehensweise bei Delikt-/Schadensfällen enthält.[4] Schadensfälle sind nicht planbar – planbar ist dagegen die Reaktion auf derartige Ereignisse.

Insbesondere kleinere und mittlere Kreditinstitute verfügen i.d.R. über vergleichsweise wenig eigene Erfahrung im Umgang mit dolosen Handlungen und Unregelmäßigkeiten, die durch eigene Mitarbeiter und/oder externe Täter verursacht wurden.[5] Dies liegt zumeist in einer in der Vergangenheit bisher nur geringen Anzahl bekannt gewordener bzw. aufgedeckter Fälle im eigenen Unternehmen begründet. Hierdurch wird eine

[2] Vgl. hierzu vertiefend die Ausführungen von Jackmuth/de Lamboy/Zawilla zum ganzheitlichen Fraud Management in Kreditinstituten sowie von Jackmuth zur Umsetzung der gesetzlichen Anforderungen an „Interne Sicherungsmaßnahmen".

[3] Vgl. vertiefend Bédé, A., 2012, Krisenmanagement im Unternehmen, S. 839 ff.

[4] Aufsichtsrechtliche Pflicht gemäß „Auslegungs- und Anwendungshinweisen der Deutschen Kreditwirtschaft (DK) zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen", Stand 16.12.2012", S. 69 f. Die BaFin hat diese Leitlinien mit ihrem Rundschreiben 1/2012 (GW) vom 06.03.2012 als „Verwaltungspraxis" anerkannt, vgl. hierzu vertiefend den Beitrag von Ackmann zu den regulatorischen Grundlagen bei der Bekämpfung „sonstiger strafbarer Handlungen".

[5] Zur besseren Lesbarkeit wird im Folgenden für „Mitarbeiter und/oder externe Täter" ausschließlich der Ausdruck „Täter" verwendet.

„gefühlte Sicherheit“ erzeugt und die vorhandenen Risiken z.T. erheblich unterschätzt.[6] Dies hat u.a. zur Konsequenz, dass in vielen Kreditinstituten lange Zeit weder angemessene aufbau- und ablauforganisatorische Rahmenbedingungen zur Verhinderung bzw. Aufdeckung von Fraud implementiert wurden, noch entsprechend ausreichende Regelungen für die Behandlung von bekannt gewordenen Fraud-Fällen vorhanden sind.

Bei Auftreten von Unregelmäßigkeiten bzw. nennenswerten Schadensfällen werden i.d.R. im Rahmen des Delikt-/Schadensfallmanagements bankinterne Sonderprüfungen oder Ermittlungen eingeleitet. Diese werden (bisher) zumeist von der Internen Revision, teilweise auch von den Bereichen Compliance, Security oder – sofern vorhanden – einer eigenständigen Organisationseinheit für Fraud Management des betroffenen Kreditinstitutes bzw. zumindest unter ihrer Federführung vorgenommen. Die genaue Vorgehensweise hängt davon ab, wie die entsprechenden Zuständigkeiten im Unternehmen geregelt sind.[7] Sonderuntersuchungen gehören für die Interne Revision zu den außerplanmäßigen Prüfungen, die diese aufgrund besonderer Vorkommnisse bzw. aufgrund von Aufträgen der Geschäftsleitung durchführt.

Mit der Ausweitung der Zuständigkeit des Geldwäschebeauftragten auch auf „sonstige strafbare Handlungen“ gemäß § 25c Abs. 9 KWG und den ergänzenden „Auslegungs- und Anwendungshinweisen der Deutschen Kreditwirtschaft (DK) zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen“, Stand 16.12.2011“, werden sich die Verantwortlichkeiten zukünftig gegebenenfalls verlagern.[8] Ungeachtet dessen bleibt die zwingende Notwendigkeit bestehen, derartige Fälle konsequent und professionell zu managen.

Dieser Beitrag gibt einen Überblick über die – unabhängig von der Größe eines Kreditinstitutes – grundsätzliche professionelle Vorgehensweise bei Bekanntwerden von Unregelmäßigkeiten oder Delikt-/Schadensfällen (Fraud-Bearbeitung), über die zahlreichen Einzelkomponenten sowie über die internen und externen Schnittstellen bei einer

[6] Vgl. vertiefend Jackmuth/de Lamboy/Zawilla zum ganzheitlichen Fraud Management in Kreditinstituten sowie Jackmuth, H.-W./de Lamboy, C./Zawilla, P., 2012, Ganzheitliches Fraud Management und der Schlüsselfaktor Mensch, S. 4 ff.

[7] Vgl. hierzu den Beitrag von Jackmuth zur Umsetzung der gesetzlichen Anforderungen an „Interne Sicherungsmaßnahmen“ sowie Zawilla, P., 2012, Strategische Komponenten im Fraud Management, S. 247 ff. sowie 262 ff.

[8] Vgl. ausführlich die Beiträge von Ackmann zu den regulatorischen Grundlagen bei der Bekämpfung „sonstiger strafbarer Handlungen“ sowie von Jackmuth zur Umsetzung der gesetzlichen Anforderungen an „Interne Sicherungsmaßnahmen“.

bankinternen Sonderuntersuchung bzw. Deliktprüfung[9] (Delikt-/Schadensfallmanagement). Dabei werden im Folgenden zunächst allgemeine Rahmenbedingungen für unternehmensinterne Sonderuntersuchungen, wie (aufsichts-)rechtliche Vorgaben, Ausgangssituationen sowie organisatorische Aspekte aufgegriffen. Anschließend wird ein strukturierter Reaktionsplan vorgestellt sowie dessen einzelne Phasen detailliert beschrieben. Der beschriebene Reaktionsplan hat sich in vielen Fällen praktisch bewährt und stammt aus eigenen Erfahrungen.

2 Allgemeine Rahmenbedingungen für unternehmensinterne Sonderuntersuchungen/Ermittlungen im Delikt-/Schadensfall

2.1 (Aufsichts-)Rechtliche Rahmenbedingungen zur Behandlung von Fraud-Fällen in Kreditinstituten

Eine professionelle sowie vollständige Aufdeckung, Aufklärung und Aufarbeitung von bekannt werdenden Unregelmäßigkeiten sollte schon allein im ureigenen Interesse einer Geschäftsleitung eines Unternehmens sowie deren Anteilseigner liegen; zudem bestehen für die Geschäftsleitung auch grundsätzliche Pflichten, sich einen Überblick über alle relevanten Sachverhalte im Unternehmen zu verschaffen.[10] Aus der Aufarbeitung heraus gilt es, Erkenntnisse zu gewinnen und entsprechende Maßnahmen abzuleiten, so dass derartige Fälle in der Zukunft vermieden werden können. Hieraus sollten auch immer Überlegungen zur Optimierung bzw. Weiterentwicklung des Internen Kontrollsystems (IKS) angestellt werden.

Aus den (branchenübergreifenden) gesetzlichen Regelungen lässt sich dies auch von bestehenden Sorgfaltspflichten und Verantwortlichkeiten der Geschäftsleitung ableiten, die in den jeweiligen Gesetzen für die einzelnen Unternehmensrechtsformen festgelegt sind.[11]

Darüber hinaus bestehen für Kreditinstitute noch erweiterte bzw. detaillierte gesetzliche bzw. aufsichtsrechtliche Vorgaben zum Umgang mit „sonstigen strafbaren Handlungen“

[9] Zur besseren Lesbarkeit wird im Folgenden für „Sonderuntersuchung bzw. Deliktprüfung“ ausschließlich der Ausdruck „Sonderuntersuchung“ verwendet.

[10] Vgl. hierzu auch Minoggio, I., 2011, Interne Ermittlungen im Unternehmen, S. 1063 ff.

[11] Vgl. insbesondere § 91 Abs. 2 sowie § 93 Aktiengesetz (AktG), § 43 GmbHG-Gesetz (GmbHG) sowie § 34 Genossenschaftsgesetz (GenG).

sowie Geldwäsche und Terrorismusfinanzierung. In diesem Zusammenhang sind insbesondere auch die konkretisierenden Regelungen in den „Auslegungs- und Anwendungshinweisen der Deutschen Kreditwirtschaft (DK) zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen“ zu nennen.[12] Zudem müssen Kreditinstitute im Rahmen ihres Risikomanagements eine institutsspezifische Gefährdungsanalyse zur Verhinderung von Geldwäsche und Terrorismusfinanzierung sowie von betrügerischen Handlungen erstellen.[13]

Berufsstandspezifisch wurden ebenfalls für den Finanzdienstleistungssektor seitens der zuständigen Aufsichtsbehörde, der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), in den Mindestanforderungen an das Risikomanagement (MaRisk) für die Interne Revision von Kreditinstituten aufsichtsrechtliche Rahmenbedingungen für die Durchführung von Sonderprüfungen festgelegt.[14]

Für die Interne Revision von Unternehmen im Allgemeinen hat international das Institute of Internal Auditors (IIA) bzw. national das Deutsche Institut für Interne Revision e.V. (DIIR) Standards für die Qualifikation von Internen Revisoren sowie für die Durchführung revisorischer Tätigkeiten aufgestellt, in denen an verschiedenen Stellen auch auf die Thematik „Fraud“ explizit eingegangen wird.[15] Zudem wurde von Kopetzky auf Basis der IIA-Standards ein Vorschlag zur Strukturierung einer Sonderuntersuchung als vorbereitende Maßnahme der Internen Revision auf den „Ernstfall“ erarbeitet.[16]

Daneben hat das Institut der Wirtschaftsprüfer (IDW) in ihrem IDW-Prüfungsstandard 210 „Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung“ ebenfalls das Thema „Fraud-Aufdeckung“ thematisiert.[17]

[12] Vgl. hierzu ausführlich den Beitrag von Ackmann zu den regulatorischen Grundlagen bei der Bekämpfung „sonstiger strafbarer Handlungen“.

[13] Einzelheiten siehe BaFin-Rundschreiben 8/2005 vom 24.03.2005 „Institutsinterne Implementierung angemessener Risikomanagementsysteme zur Verhinderung der Geldwäsche, Terrorismusfinanzierung und Betrug zu Lasten der Institute gemäß §§ 25a Abs. 1 S. 3 Nr. 6, Abs. 1 a KWG, 14 Abs. 2 Nr. 2 GwG“, vgl. auch vertiefend den Beitrag von de Lamboy zur Gefährdungsanalyse für „sonstige strafbare Handlungen“ sowie Jackmuth H.-W./Zawilla, P., 2011, Gefährdungsanalyse als zentrale Erkenntnisquelle für das weitere Vorgehen und methodisches Vorgehensmodell, S. 151 ff.

[14] Vgl. BaFin-Rundschreiben 11/2010 vom 15.12.2010: „Es muss sichergestellt sein, dass kurzfristig notwendige Sonderprüfungen, z.B. anlässlich deutlich gewordener Mängel oder bestimmter Informationsbedürfnisse, jederzeit durchgeführt werden können.“

[15] IIA-Standards in ihrer jeweils aktuellen Fassung, deutscher Text in der Fassung des DIIR.

[16] Vgl. Kopetzky, M., 2010, Standard „Sonderuntersuchung“, S. 211-221.

[17] Vgl. IDW PS 210 „Zur Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung“ in der Fassung vom 09.09.2010.

Ganzheitliche Compliance-Funktion unter besonderer Berücksichtigung der Aufgabe zur Verhinderung der „sonstigen strafbaren Handlungen"

Ulrich L. Göres

1 Einleitung

§ 25c Abs. 9 S. 1 Kreditwesengesetz (KWG) fordert, dass die Funktion des Geldwäschebeauftragten und die Funktion zur Verhinderung einer „sonstigen strafbaren Handlung" i.S.d. § 25c Abs. 1 S. 1 KWG im Institut von „einer Stelle" wahrgenommen werden. Dies wird dahingehend interpretiert, dass die Funktion zur Verhinderung einer „sonstigen strafbaren Handlung" der Funktion zur Bekämpfung der Geldwäsche und damit dem Geldwäschebeauftragten i.S.d. § 25c Abs. 4 KWG unterstellt wird, der seinerseits gemäß § 25c Abs. 4 S. 3 KWG der Geschäftsleitung direkt und unmittelbar zu berichten hat.

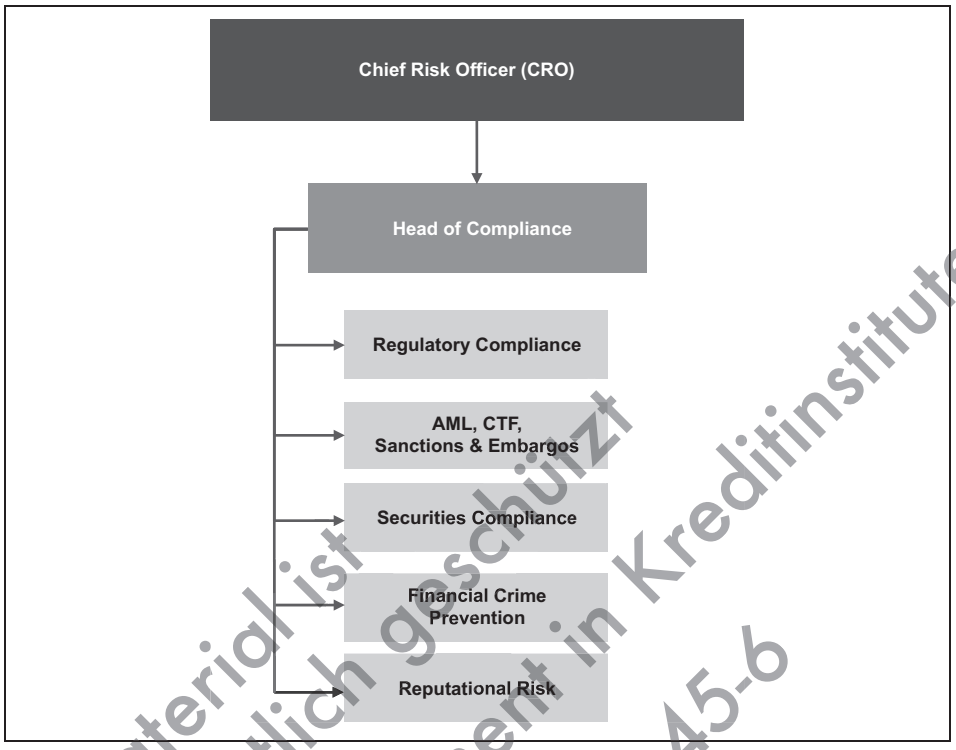
Sofern das Kreditinstitut lediglich über eine Funktion zur Bekämpfung der Geldwäsche verfügt, entstehen mit einer solchen isolierten Betrachtungsweise nur geringe Abgrenzungsprobleme. Indes spiegelt eine solche Aufstellung bereits seit geraumer Zeit nicht mehr die Wirklichkeit in der Mehrheit der Kreditinstitute wieder. Vielmehr verfügen viele mittlerweile bereits über oder sind dabei, ganzheitliche Compliance-Funktionen einzurichten, die insbesondere für die Bekämpfung der Geldwäsche (Anti-Money Laundering (AML)),[1] die Verhinderung der Terrorismusfinanzierung (Counter Terrorist Financing (CTF)), die Einhaltung von Sanktionen und Embargos (Sanctions & Embargos), die Wertpapier-Compliance (Securities Compliance),[2] die Verhinderung sonstiger strafbarer Handlungen (Financial Crime Prevention) als auch für das Management von Reputationsrisiken (Reputational Risk) zuständig sind.[3]

[1] Vgl. auch den Beitrag von Schanz zur Prävention von Geldwäsche und Terrorismusfinanzierung.

[2] Vgl. auch den Beitrag von Renz/Engl zur Abgrenzung von Fraud Management und Compliance.

[3] Siehe hierzu Abschnitte 2 und 3.

Abbildung 1: Mögliche organisatorische Struktur einer ganzheitlichen Compliance-Funktion



In dieser möglichen Struktur wird die Compliance-Funktion vom Head of Compliance (wird oftmals auch als Chief Compliance Officer (CCO) bezeichnet) geleitet, der organisatorisch, fachlich und disziplinarisch direkt dem Vorstand unterstellt ist. Häufig in der Praxis anzutreffen ist die direkte Unterstellung der Compliance-Funktion unter den Vorstandsvorsitzenden (Chief Executive Officer (CEO)), den Finanzvorstand (Chief Financial Officer (CFO)) oder den Risikovorstand (Chief Risk Officer (CRO)), da diese i.d.R. keine operativ tätigen Geschäftsbereiche verantworten. Zu bevorzugen ist die Unterstellung der Compliance-Funktion unter den CRO, da Compliance eng mit anderen Risikofunktionen, insbesondere dem Operationellen Risiko, zusammenarbeiten muss. Ferner ist zu beachten, dass die Interne Revision klassischerweise dem CEO untersteht. Ob ein und demselben Vorstandsmitglied neben der Compliance-Funktion indes auch die Interne Revision unterstellt werden kann, wird man grundsätzlich ablehnen müssen. Diese beiden Funktionen müssen gemäß § 25a Abs. 1 S. 3 KWG selbstständig nebeneinander bestehen, um eine unabhängige Kontrolle sicherzustellen.[4] Diese Zielsetzung könnte ge-

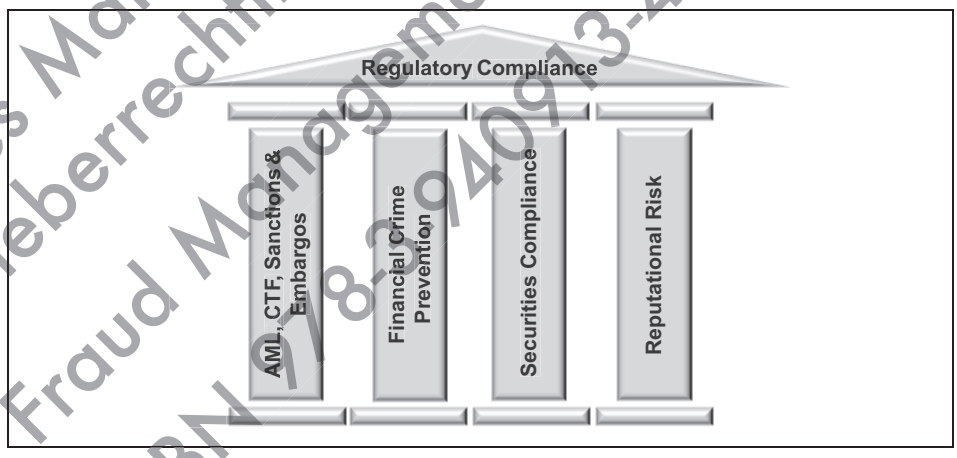
[4] Göres, U., 2012, § 33, Rn. 22 ff.

fährdet sein, wenn beide ein und demselben Vorstandsmitglied unterstellt würden; dies wäre z.B. insbesondere in Fällen möglich, in denen der Leiter der Compliance und der Leiter der Internen Revision keinen Konsens darüber erzielen können, ob die im Rahmen von Revisionsprüfungen festgestellten Moniten tatsächlich derart schwerwiegend sind oder ob diese in der Folgezeit tatsächlich behoben worden sind oder nicht. Bei gleichzeitiger Unterstellung unter ein Vorstandsmitglied müsste dieser die Entscheidung treffen. Um auch in diesen Fällen eine unabhängige Kontrolle zu gewährleisten, empfiehlt es sich, wenn schon beide Abteilungen einem Vorstandsmitglied unterstellt werden, dass in den Fällen, in denen der Leiter der Compliance und der Leiter der Internen Revision keinen Konsens erzielen können, ein weiteres Vorstandsmitglied oder der Gesamtvorstand hinzugezogen werden müssen.[5]

Häufig anzutreffende ganzheitliche Compliance-Funktionen haben folgende Unterabteilungen:

1. Regulatory Compliance,
2. AML, CTF, Sanctions & Embargos,
3. Financial Crime Prevention,
4. Securities Compliance und
5. Reputational Risk.

Abbildung 2: Schematische Darstellung einer ganzheitlichen Compliance-Funktion



[5] Göres, U., 2012, § 33, Rn. 105.

In Regulatory Compliance sind dabei die säulenübergreifenden Compliance-Aufgaben wie beispielsweise die Risikoanalyse, das Reporting (Quartals- und Jahresberichte an den Vorstand und/oder den Aufsichtsrat), der Kundenannahmeprozess, das Compliance-Training, die Methodik der Desk Reviews sowie die Wahrnehmung der Compliance-Aufgaben im Rahmen des Neue-Produkte-Prozesses angesiedelt, so dass man insoweit von einer bereichsübergreifenden oder Dachfunktion sprechen kann.

Im folgenden Beitrag wird daher folgende Fragestellungen untersucht: Welche Aktivitäten können in einer ganzheitlichen Compliance-Funktion zulässigerweise gebündelt werden?[6]

Ist die oben genannte Interpretation, d.h. Unterstellung der Funktion zur Verhinderung „sonstiger strafbarer Handlungen" unter die der Geldwäschebekämpfung (i.S.d. § 25c Abs. 9 S. 1 KWG) auch im Falle einer ganzheitlichen Compliance-Funktion notwendig oder kann § 25c KWG nicht vielmehr auch so interpretiert werden, dass § 25c Abs. 9 KWG die Eingliederung der Funktion zur Verhinderung „sonstiger strafbarer Handlungen" in die Compliance-Funktion verlangt und diese – und nicht die Funktion für die Bekämpfung der Geldwäsche – als die in § 25c Abs. 9 S. 1 KWG genannte „Stelle" anzusehen ist?[7] Besondere Bedeutung erlangt hierbei die Frage, wer in einer ganzheitlichen Compliance-Funktion gegenüber der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als Geldwäschebeauftragter i.S.d. § 25c Abs. 4 S. 1 KWG, als Wertpapier-Compliance-Beauftragter i.S.d. von der BaFin nach Konsultation der Marktteilnehmer am 07.06.2010 erstmals veröffentlichten „Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen (MaComp)"[8] sowie als Leiter der Funktion zur Verhinderung „sonstiger strafbarer Handlungen" zu benennen ist.[9]

[6] Siehe hierzu Abschnitt 2.

[7] Siehe hierzu Abschnitt 4.

[8] BaFin, 2010, MaComp, BT; siehe zu den MaComp: Bauer, F., 2010, Compliance nach den MaComp, S. 360 ff.; Becker, A./Wohlert, D., 2010, Neue MaComp, S. 160 ff.; Birnbaum, G./Kütemeier, C., 2011, Die MaComp, S. 293 ff.; Engelhart, M., 2010, Die neuen Compliance-Anforderungen der BaFin, S. 1832 ff.; Lösler, T., 2010, Die Mindestanforderungen an Compliance, S. 1917 ff.; Niermann, S., 2010, Die Compliance-Organisation im Zeitalter der MaComp, S. 400 ff.; Schäfer, H., 2011, Die MaComp, S. 45 ff.; Zingel, F., 2010, Stellung und Aufgaben von Compliance, S. 500 ff.; siehe hierzu auch Abschnitt 6.

[9] Siehe hierzu Abschnitt 6.

Systematische Betrugsprävention durch Informationsaustausch

Stephan R. Peters

1 Einleitung

Der technische Fortschritt kommt allen Menschen zugute – leider auch denen, die üble Absichten verfolgen. Betrüger nutzen moderne optische und digitale Geräte ebenso wie das Internet und andere Onlinemedien, um auf kriminelle Weise Geld oder Güter zu ergaunern. Je weiter sich die technischen Mittel entwickeln, desto besser können Täter Dokumente fälschen und Identitäten manipulieren. Die zweifelhaften Ergebnisse dieses Fortschritts bekommen Finanzinstitute und deren Kunden immer wieder zu spüren, wenn sie feststellen, Opfer von Betrügern geworden zu sein. Doch hier können Finanzinstitute[1] eine effektivere Betrugsprävention betreiben und das eigene Risikomanagement optimieren, wenn sie die Angebote von Kreditbüros und Auskunfteien besser nutzen.

Banken und Leasinggesellschaften profitieren seit Jahren von der rasanten Entwicklung des technischen Fortschritts und den dadurch entstehenden neuen Möglichkeiten und Anwendungen. Allein durch den Einsatz von Onlinekommunikationsmitteln konnten die Finanzinstitute ihre Prozesse deutlich automatisieren und Kosten senken. Finanzierungen werden infolge der Automatisierung wesentlich effizienter als in der Vergangenheit abgewickelt, Kreditgeber bearbeiten Anfragen immer rascher. Dies spiegelt sich auch im kräftigen Wachstum des Online-Bankings wider. Im Laufe des vergangenen Jahrzehnts gewannen elektronische Bankgeschäfte bei Privatkunden eine immer größere Akzeptanz. Im Jahr 2000 erledigten laut dem Bundesverband deutscher Banken erst 11% der Deutschen ihre Bankgeschäfte online, 2011 waren es bereits 44%.[2]

Doch die Industrialisierung und Automatisierung von Geschäftsprozessen sowie die zunehmend anonymen Kontakte zwischen Finanzinstitut und Kunde erhöhen auch die Gefahr von Manipulationen. Täter können durch die rasant gestiegenen technischen Möglichkeiten Dokumente qualitativ besser fälschen oder in den Online-Verkehr von Privatpersonen und Unternehmen eindringen. Auch jenseits der Finanzdienstleistungsbranche ist das Internet zu einem zentralen Instrument für Wirtschaftskriminelle geworden. Die Zahl der registrierten Fälle von Online-Kriminalität hat sich mit dem Anstieg von 2.683 im Jahr 2004 auf 31.083 im Jahr 2010 mehr als verzehnfacht.[3] Somit spielte 2010 bei mehr als jedem vierten Fall von Wirtschaftskriminalität das Internet eine Rolle.

[1] Zur besseren Lesbarkeit wird im Folgenden der Begriff Finanzinstitut synonym für Kreditinstitut und Finanzdienstleistungsinstitut verwendet.

[2] Vgl. Bundesverband deutscher Banken, 2011, Fakten und Zahlen aus der Kreditwirtschaft, S. 15.

[3] Vgl. Bundeskriminalamt, 2010, Wirtschaftskriminalität Bundeslagebild, S. 10; Bundeskriminalamt, 2008, Wirtschaftskriminalität Bundeslagebild, S. 11.

Der überwiegende Anteil der Delikte mit Internetkontakt entfiel wie schon in den Vorjahren mit 28.262 Fällen auf den Bereich Wirtschaftskriminalität bei Betrug. Insgesamt verzeichnete die Polizeiliche Kriminalstatistik (PKS) 65.648 Fälle von Wirtschaftskriminalität bei Betrug, unabhängig von der Art der Durchführung.[4] Die Zahl der Fälle von Anlage- und Finanzierungsdelikten entwickelte sich uneinheitlich. Die PKS erfasst unter diesem Oberbegriff

- alle Deliktformen im Zusammenhang mit der Vermittlung, Erlangung und Gewährung von Krediten,
- sämtliche Erscheinungsformen der Scheck- oder Wechselreiterei, der Fälschung von Geldmarktinstrumenten und
- Straftaten in Verbindung mit dem Bankgewerbe sowie nach dem Wertpapierhandelsgesetz (WpHG).

2004 betrug die Gesamtzahl der Fälle von Anlage- und Finanzierungsdelikten 12.127 und sechs Jahre später (2010) fast identische 12.174.[5] Dieser Konstanz der Fallzahlen steht eine deutliche Zunahme des durchschnittlich registrierten Schadens je Delikt gegenüber. 2010 belief er sich auf rund 76.000 EUR. Einerseits erbeuten Täter pro Delikt also höhere Beträge. Andererseits schauen die Banken seit einigen Jahren noch genauer hin und decken dadurch auch mehr und größere Betrugsdelikte auf als in der Vergangenheit.

2 Situation der Finanzinstitute angesichts krimineller Bedrohungen

2.1 Betrugsarten

Finanzinstitute und Warenkreditversicherungen (WKV) sehen sich im Wesentlichen mit fünf Betrugsarten konfrontiert:

- Identitätsbetrug
- Bonitätsbetrug
- Unterschlagungstatbeständen
- Warenkreditbetrug
- Zahlungsverkehrsbetrug

[4] Bundeskriminalamt, 2010, Wirtschaftskriminalität Bundeslagebild, S. 6.

[5] Bundeskriminalamt, 2010, Wirtschaftskriminalität Bundeslagebild, S. 11; Bundeskriminalamt, 2008, Wirtschaftskriminalität Bundeslagebild, S. 11.

Zum Identitätsbetrug zählen die Übernahme der Identität einer anderen Person, also der Diebstahl einer existierenden Identität, sowie der Aufbau einer fiktiven Identität. Als Instrument dient in beiden Fällen zumeist ein gefälschter oder gestohlener Ausweis.[6] Der kommt beispielsweise beim Betrug im Rahmen des Post-Ident-Verfahrens zum Einsatz, bei dem Mitarbeiter der Deutschen Post – Filialmitarbeiter, aber auch Briefzusteller – Empfänger identifizieren.

Beim Bonitätsbetrug manipulieren Täter bonitätsrelevante Unterlagen. Sie fälschen Gehaltsbescheinigungen, Kontoauszüge, Verträge oder andere Dokumente mit dem Ziel, die eigene Bonität zu schönen. Ein Indiz für Bonitätsbetrug sind z.B. auffallend viele gleichartige Abrechnungen oder Abrechnungssysteme, die sich einer Person oder einem Personenkreis zuordnen lassen.

Solche Machenschaften steigern sich so weit, dass sich Betrüger bzw. Betrügerbanden den Mantel einer GmbH bzw. einer Limited geben, um auf diesem Weg Kredit- oder Leasinggeschäfte über hohe Beträge abzuschließen.

Unter dem Deckmantel von Gesellschaften, v.a. von GmbHs, können Betrüger die eigene Bonität schönen. Der Weg dahin führt häufig über einen personellen Wechsel in der Geschäftsführung. Die Täter, die einen GmbH-Mantel übernehmen, können den bisherigen Bonitätsindex des Unternehmens zunächst nutzen, indem sie den alten Geschäftsführer, der diese Funktion tatsächlich abgegeben hat, nicht aus dem Handelsregister streichen lassen. Daneben tragen sie einen neuen Geschäftsführer ein. Die Hausbanken werden über den De-facto-Wechsel in der Geschäftsführung möglichst lange im Unklaren gelassen. In der Zwischenzeit nutzen die Betrüger die weiterhin positive Auskunft einer Auskunftei über dieses Unternehmen, dessen positive Bankauskunft der Hausbank und die vorhandene positive Bilanz, um neue Kredit- und Leasinggeschäfte anzubahnen und abzuschließen. Anlässe für die Finanzierung sind häufig eine Modernisierung des Fuhrparks, ein Ausbau des Außendienstes oder neue Geschäftsfelder.

Damit die finanzierenden Banken bzw. Leasinggesellschaften die Finanzierungsanfragen der Betrüger nicht zu genau prüfen, verteilen die Täter das angestrebte Gesamtvolumen auf verschiedene Finanzinstitute. Ihr Risiko ist dabei gering. Selbst wenn ein Kredit- oder Leasinggeber recherchiert, müssen die Betrüger i.d.R. höchstens eine Ablehnung des Finanzierungsantrags fürchten und werden kaum weiter verfolgt. Gelingt es ihnen, Vermögenswerte zu erlangen, verschieben sie diese schnell und verkaufen dann die GmbH

[6] Vgl. auch den Beitrag von Hessel/Heuser zum Erkennen von ge- und verfälschten Ausweisdokumenten und Aufenthaltstiteln.

Research-Systeme für Geldwäsche, Terrorismusfinanzierung und Fraud

Jürgen Krumrain/Steffen Munz/Karin Ohnesorge

1 Bedeutung moderner Präventionssysteme im Kampf gegen Wirtschaftskriminalität

Die Bedeutung moderner Präventionssysteme im Kampf gegen Wirtschaftskriminalität liegt in der hohen Kosteneffizienz, mit der sie dem steigenden Risiko zum Schutz der Geschäftstätigkeit von Finanzinstituten, deren Kundenvermögen und Reputation begegnen. Sie ermöglichen verlorenes Vermögen zurückzuerlangen und zukünftige Verluste zu verhindern.

Als wirksame und transparente Risikoabsicherung unterstützen und entlasten sie die von Compliance-Richtlinien betroffenen Geschäftsprozesse, beginnend bei der Kundenannahme bis hin zur Abklärung auffälliger Sachverhalte. Sie automatisieren die Risiko-Klassifizierung von Geschäftsfeldern, Kunden, Geschäftspartnern, Mitarbeitern und Produkten und überwachen kontinuierlich alle Geschäftsbeziehungen und Finanztransaktionen.[1]

Der gezielte Einsatz moderner Präventionssysteme ermöglicht die nachhaltige Bekämpfung und zeitnahe Unterbindung von illegalen Handlungen. Dabei ist es unerheblich, welche Tatbestände den illegalen Handlungen zugrunde liegen. Die Bekämpfung und Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen" wie Betrug, Korruption oder die Einhaltung von Sanktionen und Embargos erfolgt in zeitgemäßen Präventionssystemen für alle Tatbestände gleichermaßen über flexible regelbasierte Mustererkennung. Zur Vereinfachung und besseren Lesbarkeit wird im Folgenden der Begriff „Betrug" mit den sonstigen „strafbaren Handlungen" gleichgesetzt. Eine erfolgreiche Präventionsstrategie erfordert zwingend eine fortlaufende Anpassung an neue Muster illegalen Handelns. Präventionssysteme der neuen Generation bieten daher einfache Verfahren für Regeländerungen und unterstützen diese idealerweise durch statistische Verfahren und Simulationen. Zur Aufdeckung interner Betrugsmuster erlauben sie zudem die datenschutzkonforme Überwachung und Bearbeitung von pseudonymisierten oder anonymisierten Mitarbeiterdaten.[2]

Als mandantenfähige und mehrsprachige Baukastensysteme lassen sie sich konzernweit in Compliance-Prozesse und beliebige technische Infrastrukturen integrieren. Auf dem Markt international etablierte und bewährte Compliance-Systeme garantieren zudem

[1] Vgl. auch den Beitrag von Schanz zur Prävention von Geldwäsche und Terrorismusfinanzierung.

[2] Vgl. auch den Beitrag von Polenz zu Grenzen von Fraud Detection im Lichte der aktuellen Datenschutzbestimmungen.

niedrige False-Positive-Raten und eine hohe Performance bei der Verarbeitung von Massendaten. Sie sind somit bestens gerüstet für den prognostizierten Anstieg von Betrugsattacken und Finanztransaktionen.

2 Systemeinsatz im fachlichen Geschäftsprozess

Im Gegensatz zum Geldwäsche- und Terrorismusrisiko ist das Risiko „sonstiger strafbarer Handlungen" weitaus komplexer. Es geht nicht „nur" um das Einschleusen von inkriminierten Geldern in den Bankkreislauf oder die Finanzierung von Terrorismusaktivitäten. Die handelnden Personen, die Betrugsfelder und die Betrugsmuster sind deutlich umfangreicher und vielfältiger.

Während sich die Risikoarten Geldwäsche und Terrorismusfinanzierung auf die Kunden des Kreditinstituts konzentrieren, rücken bei Betrug die eigenen Mitarbeiter, Kontrahenten, Lieferanten, Geschäftspartner oder auch fremde Personen ins Blickfeld. Im Weiteren wird zur Vereinfachung der Begriff „Partner" als Obergriff für Kunden, Kontrahenten, Lieferanten und Geschäftspartner benutzt.

Die Betrugsfelder erstrecken sich neben den eigentlichen Bankdienstleistungen auch auf die Gebiete der Beschaffung, insbesondere der Beschaffung von IT, auf den Einkauf von Dienstleistungen, auf das Rechnungswesen und auf Baumaßnahmen – um nur die wichtigsten zu nennen. Die Angriffspunkte und Betrugsmuster sind entsprechend vielfältig:[3]

- Kreditbetrug;
- Anlagebetrug;
- Internetbetrug;
- Betrug im Wertpapierhandel;
- Korruption;
- Diebstahl;
- Steuerbetrug;

[3] Vgl. auch die Beiträge von Altenseuer zu Manipulationen im Vertrieb, Kaup/Zawilla zu typischen Fraud- und Manipulationspraktiken, de Lamboy zur Gefährdungsanalyse für „sonstige strafbare Handlungen" und Neuber zu Fraud-Praktiken im Bauspar- und Zuträgergeschäft.

Die vom Gesetzgeber geforderte Systemunterstützung bei der Überwachung von Betrugsrisiken muss an vielen Punkten ansetzen: zu allererst bei den Kernbanksystemen und der Überwachung von Konten. Letzten Endes resultieren die meisten Betrugsfälle in Geldbewegungen zugunsten des Betrügers. Auch die Betrugsfälle in der Beschaffung und im Rechnungswesen spiegeln sich in Kontobewegungen wieder, vornehmlich auf internen Konten.

Im Rahmen der Gefährdungsanalyse werden die Betrugsfelder und die Betrugsmuster entsprechend dem Geschäftsportfolio des Kreditinstituts dargestellt. Die nach Eintrittswahrscheinlichkeit und Schadenshöhe klassifizierten Risiken erlauben auch bei der Systemunterstützung einen risikobasierten Mitteleinsatz. Für die Untersuchung von Massendaten z. B. im Retail-Geschäft sind moderne IT-Systeme unumgänglich.[4]

Hinweise auf betrügerische Handlungen lassen sich auf drei wesentliche Grundmuster zurückführen:

- untypisches Verhalten, gemessen am bisherigen Verhalten des Partners oder Mitarbeiters oder gegenüber einer Vergleichsgruppe;
- nicht erwartetes Verhalten, gemessen an den Aussagen bei der Geschäftseröffnung;
- regelwidriges Verhalten.

Hier können Systeme ansetzen und im Idealfall die kriminelle Handlung verhindern oder zumindest aufdecken. In den ersten beiden Punkten spielt das Know-Your-Customer- (KYC), das Know-Your-Employee- (KYE) und das Know-Your-Supplier-Prinzip (KYS) eine entscheidende Rolle. Damit Systeme dieses Prinzip verwenden können, muss das Wissen über den Partner oder Mitarbeiter elektronisch vorliegen, aber v.a. in strukturierter und klassifizierender Weise, z. B. in Form von Kennzahlen. Abgeleitet aus dem Wissen über den Partner kann man eine Risikoeinschätzung vornehmen, die alle Partner in die vier Klassen unterteilt:[5]

- geringes Risiko;
- normales Risiko;
- erhöhtes Risiko;
- stark erhöhtes Risiko.

[4] Vgl. auch die Beiträge von Jackmuth/Parketta zu Methoden der Datenanalytik und Ackmann zu den regulatorischen Grundlagen bei der Bekämpfung „sonstiger strafbarer Handlungen".

[5] Vgl. auch den Beitrag von de Lamboy zur Gefährdungsanalyse für „sonstige strafbare Handlungen".