bank&compliance

Dirk Scherp

Fraud Management

Abwehr von Kriminalität in der Organisation von Kreditinstituten und Finanzdienstleistern

2. Auflage

bank&compliance

Fraud Management

2. Auflage

Abwehr von Kriminalität in der Organisation
von Kreditinstituten und Finanzdienstleistern

Dirk Scherp

Copyright 2015 by Bank-Verlag GmbH
Postfach 45 02 09 · 50877 Köln

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verbreitung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Bank-Verlag GmbH unzulässig und strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung, Mikroverfilmung sowie die Einspeicherung und Verarbeitung in elektronischen Systemen.

Der Inhalt wurde mit größtmöglicher Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität des Inhalts übernimmt der Verlag keine Haftung.

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Art.-Nr. 22.463-1500
ISBN 978-3-86556-457-3

Inhaltsverzeichnis

Vorwort 1

A Die Bekämpfung strafbarer Handlungen im Institut 3

1. Die Aufgabe im Überblick 3
1.1 Entstehung und Entwicklung der Norm 8
1.2 Die bisherige Regelung: § 25c KWG (alt) 12
1.3 Prävention und Ermittlung 15
1.4 Betrügerische Handlungen, Fraud und sonstige strafbare Handlungen 19

2. Die aktuelle Fassung von § 25h KWG 21
2.1 Der Gesetzestext: Überblick 21
2.2 Definition „strafbare Handlungen“ 24
2.3 Die Pflichten im Einzelnen 31
2.4 Sicherungssysteme 35
2.5 Systemkontrollen 39
2.6 Die Untersuchungspflicht 41

3. Untersuchungspflicht und Anzeige 49
3.1 Untersuchungspflichtige Sachverhalte 49
3.2 Keine Anzeigepflicht 50
3.3 Die Strafanzeige 54
3.4 Weitere Entscheidungskriterien 56
3.5. Aufzeichnungspflichten 59
3.6 Informationsaustausch und Datenschutz 63

3.7 Organisationspflichten 65

4. Weitere Organisationsfragen, Kontrollen und Prüfungen 69
4.1 Prüfungsberichtsverordnung 69
4.2 Organisationshinweise 74

B Definition und Beispiele strafbarer Handlungen im Institut 77

1. Erscheinungsformen und Kriminologie typischer Wirtschaftsstraftaten 77
1.1 Zur Kriminologie der Betrugsdelikte 77
1.2 Die Legaldefinition von Wirtschaftskriminalität 79

2. Das Leipziger Verlaufsmodell wirtschaftskriminellen Handelns 82

3. Das Fraud-Triangle 85

4. Kriminalstatistik und Lagebild 92

5. Mehr Empirie: Die Untersuchungen von Wirtschaftsprüfern 96

6. Fraud: Definitionen 101

7. Tatbestände des Strafrechts – ein Überblick 103
7.1 Betrug – § 263 StGB 104
7.2 Subventionsbetrug – § 264 StGB 109
7.3 Kapitalanlagebetrug – § 264a StGB 110
7.4 Kreditbetrug – § 265b StGB 111
7.5 Untreue – § 266 StGB 111

8. Spezialmaterien 116
8.1 Korruption 116

8.2 Kapitalmarktstrafrecht 125
8.3 Ordnungswidrigkeiten 129

9. Die Täter 133

10. Beispielsfälle: Betrug mit Kapitalanlagen und Schneeballsysteme 144
10.1 K1 Invest – die deutsche Variante 146
10.2 Die Lehren ziehen – Betrug mit Kapitalanlagen ist vermeidbar 149

C Prävention 153

1. Überblick 153
1.1 Gefährdungsanalyse 154
1.2 Methodik der Gefährdungsanalyse 157

2. Schriftlich fixierte Ordnung 173

3. Einzelmaßnahmen 194
3.1 Das Vier-Augen-Prinzip 194
3.2 Hinweisgebersysteme und Ombudsmann 196
3.3 Plausibilitäts-Checks 203
3.4 KYC-Prinzip 206
3.5 Integrity-Verträge 210

4. Präventive Datennutzung und Monitoring 213
4.1 Datennutzung zu präventiven Zwecken 213
4.2 Monitoring 216

D Ermittlungen 219

1. Interne Ermittlungen 219
1.1 Festlegung des Untersuchungsziels und Planung 223

1.2 Organisation interner Ermittlungen und externer Unterstützung 229
1.3 Verdacht 237
1.4 Kriminalistik 244

2. Einzelne Ermittlungsmethoden 248
2.1 Befragung von Mitarbeitern 248
2.2 Befragungsmethoden 256
2.3 Fragetechnik und Strategie 259

3. Sonderuntersuchungen und Datenschutz 264
3.1 Einleitung 264
3.2 Auftragsdatenverarbeitungsvertrag 266
3.3 Übermittlung an einen Dritten 267
3.4 Verarbeitung und Nutzung der Daten 268
3.5 Rechtliche Grundlagen der Untersuchung 269
3.6 Straftatermittlungen nach § 32 BDSG 273
3.7 Besonderheiten beim E-Mail-Verkehr 275
3.8 Private Nutzung der E-Mail 277

4. Die Rolle der Ermittlungsbehörden 279
4.1 Polizei und Staatsanwaltschaft – Befugnisse im Überblick 279
4.2 Durchsuchung im Unternehmen 284
4.3 Beispiel einer Organisationsanweisung 291
4.4 Auskunftsersuchen 297

5. Schadenersatz: Asset Recovery 298

Literaturverzeichnis 301

Stichwortverzeichnis 311

Vorwort

Die regulatorischen Rahmenbedingungen haben sich seit der ersten Auflage dieses Buches in schneller Folge und mehrfach geändert. Das hat nicht nur dazu geführt, dass der vormalige § 25c KWG jetzt in § 25h KWG verankert ist, sondern auch inhaltliche und terminologische Klarstellungen zur Folge, die in den Auslegungs- und Anwendungshinweisen der Deutschen Kreditwirtschaft zum Ausdruck gekommen sind. Dabei ist auch die mit der Bekämpfung von „sonstigen" Straftaten in enger Beziehung stehende Geldwäscheprävention einem ständigen Wandel unterworfen. Mehrere, zum Teil recht abseitige Gesetze, haben hier Änderungen herbeigeführt und die Vierte EU-Geldwäscherichtlinie ist auf der Zielgeraden zu ihrer Verabschiedung. Auch die MaRisk-Novelle aus dem Jahr 2012 hat Einfluss auf die Organisation der Kriminalprävention genommen, da Zuständigkeiten zum Teil angepasst, zum Teil neu definiert werden mussten.

Diese Änderungen, die in vielen betroffenen Häusern zu einer Korrektur der gesamten Compliance-Architektur geführt haben dürften, haben wir in der 2. Auflage so weit wie möglich berücksichtigt und eingearbeitet. Konstruktive Kritik aus der Leserschaft haben wir aufgenommen und versucht, umzusetzen: noch weniger juristische Dogmatik, noch mehr praktikable Anwendungshinweise waren der Leitgedanke dieser aktualisierten Auflage.

Daher kann das Buch im Einzelfall nicht das vertiefende Nachschlagen in den Rechtskommentaren oder der Fachliteratur sowie die Einholung von Rechtsrat ersetzen.

Noch hat die Eindämmung der Finanzkriminalität nicht überall die Bedeutung und die Anerkennung erlangt, die ihr gebührt. Schaden vom eigenen Institut abzuwenden; Straftäter, auch wenn sie aus den eigenen Reihen kommen, zu entlarven und ihrem Tun Einhalt zu gebieten, sind eminent wichtige

Aufgaben im Umfeld der Finanzbranche, um Ansehen und Vertrauen in der Öffentlichkeit zurückzugewinnen. Das wird aber nur gelingen, wenn es dabei stets professionell und rechtmäßig zugeht und die Grenzen des Rechts und der Verhältnismäßigkeit gewahrt werden. Es würde mich freuen, wenn dieses Buch dazu einen Beitrag leisten kann.

Frankfurt am Main, im Mai 2015

Dirk Scherp

A Die Bekämpfung strafbarer Handlungen im Institut

1. Die Aufgabe im Überblick

Mancher Leser dieses Buches mag schon einmal eine E-Mail wie diese bekommen haben:

> Lieber Freund, Mein Name ist Steven Erwin. Ich arbeite mit einem Finanzierungs Haus hier in den Niederlanden. Während meiner letzten Sitzung und Prüfung der Bankkonten in unserer Bank, meine Abteilung fand ein ruhendes Konto mit einer enormen Summe von US $ 55,500,000.00, die von einem verstorbenen Herrn Williams aus England vor abgelagert wurde sein Tod. Aus unserer Untersuchung hatte er keine nächsten Angehörigen, diese Mittel zu erreichen. Nach Ansicht der niederländischen Bankenregulierung nur ein Ausländer als nächsten Angehörigen stehen, angesichts der Tatsache, dass der Hinterleger war ein nicht-Niederländisch. Ich brauche Ihre Erlaubnis, als Partner unserer verstorbenen Kunden zu stehen, so dass die Mittel freigegeben und sofort auf Ihr Bankkonto überwiesen. Am Ende der Transaktion 40% wird für Sie sein, und 60% für mich und meine Kollegen. Ich arbeite noch an der Finanzhaus und das ist der Grund, warum ich noch eine zweite Partei mit zu arbeiten. Ich habe in meinem Besitz aller erforderlichen Unterlagen zu haben, diese Transaktion erfolgreich durchgeführt. Weitere Informationen werden nach dem Eingang der Ihre prompte Antwort zur Verfügung gestellt werden. Beachten Sie auch, dass diese Transaktion ohne Risiko, ist alles, was ich brauche deine Ehrlichkeit und Vertrauen. Bitte antworten Sie mir mit Ihren privaten E-Mail (für vertrauliche Gründen), so dass ich Ihnen mehr Details und erläutern die Verfahren der Vorschlag an Sie. Bitte bitte antworten zurück zu mir dringend obwohl meine private E-Mail (steven.erwins@aim.com) Mit freundlichen Grüßen Steven Erwin

Ich habe genau diese E-Mail vor wenigen Tagen bekommen, als ich mit der Bearbeitung der zweiten Auflage befasst war.

„Das ist doch zu dumm“, werden Sie vermutlich denken, verehrter Leser – „da fällt doch wirklich niemand mehr drauf rein“.

Oder Sie werden sich fragen, ob das nicht eher etwas mit Geldwäsche zu tun hat, als mit Betrug und Prävention.

Und dennoch: Die Absender würden solche E-Mails nicht massenweise versenden, wenn sie nicht doch den einen oder anderen Erfolg verbuchen könnten. Das Bundeskriminalamt berichtet in seinem Jahresbericht 2013 der Zentralstelle für Verdachtsmeldungen von 3.493 Meldungen im Zusammenhang mit dem Phänomen „Financial Agents“, das sind rund 18 Prozent des gesamten Verdachtsmeldeaufkommens (vgl. BKA, 2013).

Seit 2006 wird dieses Phänomen beim BKA registriert und gesondert ausgewiesen. Damals waren es noch 285 Meldungen, die sich bis 2011 kontinuierlich auf 3.992 Meldungen gesteigert haben.

Nicht wenige der Betroffenen werden auch auf die üblichen Forderungen der E-Mail-Verfasser reagiert haben und Geld zur „Vorfinanzierung“ der Transaktion überwiesen haben, das sie dann, ebenso wie die angeblichen 40 Prozent der Gesamtsumme, nie wiedergesehen haben. Die Dunkelziffer dürfte angesichts des oben registrierten Meldeverhaltens der Institute aus der Finanzbranche noch wesentlich höher liegen, zumal viele Betrugsopfer sich scheuen, von sich aus die Ermittlungsbehörden einzuschalten.

Aber was hat das alles mit der Verpflichtung der Institute zu tun, gemäß § 25h KWG Vorkehrungen gegen „sonstige“ Straftaten zu treffen, die das Vermögen des Instituts schädigen können?

Es hat mindestens so viel damit zu tun, wie die Schlagzeilen über die Verurteilung einiger Prominenter wegen Wirtschafts- und Steuerdelikten oder die Meldung in der FAZ vom 06. Januar 2015 (S. 29): „Anklageschrift gegen S&K-Gründer offenbar fertig".

In der Meldung wird über die mutmaßlichen Straftaten bei der Immobilieninvestmentgruppe S&K berichtet, deren Inhaber und Betreiber verdächtigt werden, mehrere tausend Anleger um mehr als 100 Mio. € – „wenn nicht sogar um das Doppelte dieser Summe" – betrogen zu haben.

Meldungen wie diese deuten darauf hin, dass sich in der justiziellen Aufarbeitung seit der Finanzkrise die Akzente verschoben haben, nicht jedoch die grundsätzlichen Gegebenheiten der Prävention gegen „sonstige strafbare Handlungen" im Institut. Der nette E-Mail-Schreiber Erwin und die S&K Finanzgruppe müssen Konten führen und geführt haben, um ihre Transaktionen abzuwickeln. Für Fonds der S&K-Gruppe wurden Depots errichtet und Verwahrstellen gefunden, Investorengelder sind sicher nicht in bar geflossen.

Die Tathandlungen mögen komplizierter, die Tatzusammenhänge komplexer geworden sein. Dafür sprechen rund 1.500 Seiten Anklageschrift.

Vorstandsetagen der großen deutschen Banken sind keine terra incognita der Ermittler mehr. Die gesamte Top-Liga der deutschen Wirtschaft scheint betroffen zu sein.

Auch wenn die Wirtschaftsdelikte in Deutschland laut Kriminalstatistik geringfügig rückläufig zu sein scheinen, bleiben die Fallzahlen beim Betrug und dem Betrug mit Kapitalanlagen auf hohem Niveau. Der Untreuetatbestand des Strafgesetzbuches (§ 266 StGB) ist zur meistdiskutierten Vorschrift in den strafrechtlichen Fachblättern geworden.

Auch die in der ersten Auflage gestellten Fragen bleiben aktuell und werden durch neue Fallkonstellationen ergänzt: Ist die Finanzkrise schuld? Geben

Banker wie der „Cityboy“ den Takt an? Hat die „große Gier“ alles und jeden erfasst oder fehlt es nur an der „richtigen Corporate Governance“, einer „Ethik des Erfolgs“, an zupackendem Wertemanagement und durchsetzungsfähiger Compliance?

„Ist die Deutsche Bank eine kriminelle Vereinigung?“ (Hetzer in: Die Kriminalpolizei 1/2014, S. 26) oder handelt es sich nur um eine „Kultur des Wegsehens“? (so Der Spiegel 2/2014, S. 61).

Egal, ob Milliardenschaden in den Finanzzentren der Welt oder ungetreuer Eingriff in ein Kundenkonto bei einem örtlichen Finanzinstitut: Für das betroffene Haus entsteht ein Reputationsschaden, auch wenn der Kunde entschädigt wird. Die Bankenbranche büßt weiter Vertrauen ein, die bösen Ahnungen der Finanzkrise scheinen sich in jedem Einzelfall zu bestätigen.

Daran ändern auch Freisprüche oder mit Bußgeldzahlungen teuer erkaufte Verfahrenseinstellungen wegen „geringer Schuld“ für Führungskräfte wenig. Im Gegenteil: Die Behauptung, dass „organisierte Unverantwortlichkeit“ auch in Banken und bei Finanzdienstleistern nur durch Einführung eines Unternehmensstrafrechts mit der Möglichkeit der Verhängung von „Verbandsgeldstrafen“ gegen das betroffene Unternehmen selbst bekämpft werden könne, hat sich in der Politik bereits durchgesetzt.

Sollte das „Verbandsstrafgesetzbuch“ legislative Wirklichkeit werden, stellen sich den Präventions-Beauftragten in den Instituten bald völlig neue Herausforderungen. Die fachgerechte Umsetzung der nunmehr in den §§ 25h ff. KWG enthaltenen Präventionsvorschriften wird noch mehr als bisher einen Gesamtüberblick über das Institut, sein Geschäftsmodell und die Geschäftsorganisation verlangen, zu dem auch die sichere Beherrschung der institutsinternen Governance-Regeln und der gesellschaftsrechtlichen Erfordernisse (Wer darf was im Unternehmen? Welche Zustimmungs- und Genehmigungsprozesse sind einzuhalten?) gehören werden.

Wer im Institut Kriminalprävention verantwortet, darf die Augen nicht mehr vor „Management Override“ und pflichtwidrigen Gremienentscheiden verschließen, will er nicht selbst als Beschuldigter in den Fokus der Ermittler geraten. Ernstzunehmende Stimmen warnen im Hinblick auf die internen Ermittlungen bereits vor einem „Wettrüsten mit Strafverfolgungsbehörden“ (Eckert, in: Unternehmensjurist 4/2013, S. 35).

Insofern verschieben sich auch in der zweiten Auflage dieses Buches die Akzente: „Betrugsprävention“ ist nicht mehr genug; umfassende „Kriminalprävention“ tritt in den Vordergrund. Zwar bleibt der individuell begangene Betrug einzelner, häufig interner Täter oder kleiner Tätergruppen ein wesentliches Bedrohungsszenario in den Instituten. Doch müssen organisationsspezifische Ansätze, prozessorientierte Kontroll- und Ermittlungshandlungen und Erklärungsmuster hinzutreten, die sich von der Betrachtung des Einzelfalles (und des Einzeltäters) lösen, um erfolgreich zu sein.

Andererseits sollte den Verantwortlichen klar sein, dass sich Kriminalität nicht vollständig verhindern, bekämpfen oder gar „ausrotten“ lässt. Kriminalität ist „ubiquitär“ – das heißt, sie kann immer und überall zu Tage treten, unter allen Umständen, in allen Systemen und daher auch in jedem Unternehmen. Auch wo sie nicht zu Tage tritt, ist sie vorhanden – die Kriminologen nennen das „Dunkelfeld“.

Daher gilt: Präventionsprogramme, Compliancesysteme und Kontrollmechanismen müssen angemessen auf die Risikolage reagieren. Interne Ermittlungen haben rechtsstaatlichen Ansprüchen zu genügen.

Überzogene Überwachung verhindert keine Kriminalität, sondern zerstört das Betriebsklima und die Unternehmenskultur. Illegale Aufklärungsmaßnahmen können der Reputation des Instituts mehr schaden, als der eine oder andere Schadensfall, der durch unternehmerische Fehlentscheidung, aber nicht durch kriminelles Tun ausgelöst wurde.

Und schließlich: Überbürokratisierte Kontrollsysteme verhindern allenfalls schnelle, verantwortungsbewusste Entscheidungen, aber nicht die Begehung von Straftaten zum Nachteil des Instituts durch einen entschlossenen Täter.

Zur weiteren Annäherung an das Aufgabengebiet dient zunächst ein Blick auf die gesetzliche Entwicklung.

1.1 Entstehung und Entwicklung der Norm

§ 25h KWG hat eine längere Entwicklung hinter sich, bis die jetzt gültige Formulierung vorlag.

Mit den Gesetzespaketen zur Neuregulierung der Finanzmärkte im Jahre 2002, dem Vierten Finanzmarktförderungsgesetz und dem Finanzkonglomerategesetz wurde die Aufgabe der „Betrugsbekämpfung" in dem 1997 eingeführten § 25a KWG erstmals als „besondere organisatorische Pflicht von Instituten" gesetzestechnisch verankert und gleichrangig neben die Geldwäschebekämpfung gestellt.

Dennoch führte diese gesetzestechnische Hervorhebung der „Betrugsbekämpfung" als eigenständige Aufgabe nicht annähernd zu den organisatorischen Veränderungen und Vorkehrungen, die dem in der Geldwäschebekämpfung betriebenen Aufwand vergleichbar wäre. Erst wiederkehrende Ankündigungen von Wirtschaftsprüfern, die Organisation der „Betrugsbekämpfung" zukünftig gleichen Prüfungsmechanismen wie bei der Geldwäschebekämpfung unterziehen zu wollen und die abermalige neue Verortung der Prävention gegen „sonstige Straftaten" in § 25c KWG im Jahr 2011 als selbstständige Aufgabe, zu deren Erfüllung interne Sicherungsmaßnahmen zu ergreifen sind, führte zur verstärkten Beachtung dieser finanzwirtschaftlichen Pflichtaufgabe.

Dazu ist das Gesetz zur Umsetzung der Zweiten E-Geld-Richtlinie vom 01. März 2011 im Bundesgesetzblatt verkündet worden (BGBl. I 2011, S. 288), das mit Inkrafttreten zum 30.04.2011 den damals neuen § 25c KWG als Grundlage der Bekämpfung von Straftaten durch Institute geschaffen hat.

Mit der Neuregelung wurde eine weitgehende Gleichstellung der beiden Themenbereiche – Geldwäschebekämpfung und Kriminalitätsbekämpfung – vollzogen.

Schon durch die Neufassung des Gesetzestextes im Jahr 2008 stand nicht mehr nur der „interne Täter", der „unzuverlässige" Mitarbeiter im Blickpunkt. Vielmehr hatte seitdem die „Verhinderung von betrügerischen Handlungen" jeglichen schädigenden Angriff auf das Institut im Rahmen des angemessenen Risikomanagements möglichst zu unterbinden.

Damit rückten auch Schadhandlungen Dritter, die nicht bei einem Finanzdienstleister angestellt sind, in den erweiterten Fokus. Es galt, schädigende Handlungen dort abzuwehren, wo sich der Täter die Mechanismen oder Systeme der angebotenen Finanzdienstleistungen zunutze macht, um die Bank selbst oder, unter Ausnutzung ihrer Dienstleistungen, deren Kunden zu schädigen. Solche Angriffe Dritter, die die vorhandenen Systeme des Instituts nutzen, nehmen mit der Erweiterung automatisierter Dienstleistungsangebote stark zu.

„Phishing" und „Skimming" sind Beispiele der Schädigung des Kunden durch Missbrauch von Finanzdienstleistungen. „Phishing" bezeichnet den Missbrauch von Daten eines Internetbenutzers, die auf technischem Wege oder durch fingierte Abfragen an den Dateninhaber selbst erlangt wurden. Die Täter machen sich die kommunikativen Techniken des Internets zu eigen, fälschen elektronische Nachrichten oder ganze Webseiten und kommen dadurch in den Besitz von Benutzernamen, Passwörtern, Konto- und Kreditkarteninformationen sowie Sicherheitsmerkmalen wie PIN- und TAN-Nummern. Zumeist wird der Empfänger solcher gefälschten Nachrichten aufgefordert, geheime Zugangsdaten preiszugeben, nicht selten kommen aber auch Trojaner und Schadware zum Einsatz – die Daten werden auf dem Kommunikationsweg einfach abgegriffen. „Skimming" betrifft ebenfalls die Ausspähung von Kreditkarten- oder Debitkartendaten. Ziel der Täter ist das gleichzeitige Erlangen von PIN-Nummer des Kartennutzers und der auf dem Magnetstreifen

enthaltenen Daten. Die Magnetstreifendaten werden durch ein Lesegerät, das ohne Kenntnis des Benutzers zusätzlich am Geldautomaten angebracht wird, ausgelesen. Die PIN wird meist durch Anbringung einer Miniaturkamera erfasst, wenn der Benutzer sie eingibt.

Technische Blockaden, wie Antiskimming-Module, regelmäßige physische Untersuchungen der Automaten auf Manipulationen und Anbringung versteckter Kameras haben Abhilfe geschaffen. Die Datenübertragungssysteme sind sicherer geworden, wenn der Nutzer bereit ist, Sicherungstechniken anzuwenden. Doch unangreifbar sind sie nicht. Jeder technische Fortschritt fordert die kriminelle Gegenseite zu neuen Anstrengungen heraus, die Sicherungen zu überwinden. Auch in dieser Beziehung hat das Wettrüsten, wie unzählige Hacker-Attacken beweisen, ungeahnte Ausmaße angenommen.

In den folgenden Ausführungen können und wollen wir uns jedoch nicht mit den spezifisch technischen Erscheinungsformen und Ausprägungen betrügerischer Handlungen befassen. Eine solche Darstellung würde zu weit führen und auf technische Details und Entwicklungen eingehen müssen, die sich vorliegend nicht umfassend darstellen lassen. Die wirksame Bekämpfung IT-technisch begangener Kriminalität, mag man sie nun Cybercrime, Computerkriminalität oder Internetkriminalität nennen, ist Sache von IT-Spezialisten. Das kann und will dieses Buch nicht leisten.

Fest steht aber: Die Abwehr von kriminellen Handlungen, die unter Ausnutzung modernster Kommunikationstechnik erfolgen, ist Teil der Sicherheitsarchitektur einer Bank oder eines Finanzdienstleisters. Sie muss, unter Einbeziehung des zugehörigen Datenschutzes, in die geschäfts- und kundenbezogenen Sicherungssysteme des Instituts integriert sein und in enger Anbindung an die übrigen Maßnahmen der Geschäftsorganisation zur Verhinderung von strafbaren Handlungen funktionieren.

Auch außerhalb der technisch-manipulativen Tatbegehungsweisen sind eine Vielzahl von betrügerischen Angriffen Dritter gegen Institute und ihre Kun-

den denkbar: Anlagebetrüger richten Konten ein, um die Assets ihrer zahlungswilligen Klientel entgegenzunehmen. Stoßbetrüger brauchen Sammelkonten, um die Einzahlungen ihrer Opfer in kürzester Zeit poolen und abverfügen zu können. Nicht selten legen sie dem tausendfach versandten betrügerischen Rechnungsformular gleich den Überweisungsträger des kontoführenden Instituts bei, um bei dem Empfänger die routinemäßige und nahezu reflexhafte Zahlungsbereitschaft auszulösen.

Ungetreue Mitarbeiter brauchen Girokonten, um sich ihren selbstgewährten Zusatz-Bonus zu überweisen, wenn sie nicht gleich das Mittel der Barauszahlung am Automaten wählen, um mit der „Ersparnis von Kontogebühren" den Controller von der Richtigkeit der Vorgänge zu überzeugen.

Beispiele für den Missbrauch von Bankdienstleistungen zu betrügerischen Zwecken gibt es unzählige, einige sind exemplarisch in diesem Buch aufgeführt.

Der Schutz des Instituts und seines Vermögens (sowie der Kunden und des Kundenvermögens) ist damit zweigeteilt: Gegen Handlungen, die aus dem Institut heraus, also durch Mitarbeiter zulasten des Instituts oder des Kunden erfolgen, sind Schutzmechanismen zu implementieren. Angriffe Dritter auf das Vermögen des Instituts sind ebenfalls bestmöglich systemisch zu verhindern.

Der Schutz des Kunden und seines Vermögens ist hingegen im Gesetzestext nicht ausdrücklich erwähnt. Er ist allenfalls Reflex des Selbstschutzes, den die Institute zu leisten haben und beruht auf der Tatsache, dass Schadensersatzpflichten und Reputationsschäden drohen, wenn Kunden durch kriminelle Handlungen Dritter oder von Mitarbeitern geschädigt werden.

Daran hat inhaltlich auch die neuerliche, zweimalige Verschiebung der Vorschrift, nunmehr in § 25h KWG, nichts geändert. Nachdem die Vorschrift mit dem CRD-IV Umsetzungsgesetz kurzfristig in § 25g KWG verankert war,

wurde sie mit dem sogenannten Risikoabschirmungsgesetz vom 07.08.2013 mit Wirkung vom 30.01.2014 (Tag der Verkündung) in § 25h KWG verortet.

Mehrere Änderungen anderer Finanzmarktgesetze, zuletzt eine KWG-Änderung durch das Gesetz zur Anpassung von Gesetzen auf dem Gebiet des Finanzmarktes vom 15.07.2014, machten immer wieder redaktionelle Anpassungen erforderlich. Wesentliche inhaltliche Änderungen sind hierdurch jedoch nicht vorgenommen worden.

Gegen Angriffe Dritter auf das Vermögen des Kunden kann das Institut schutzpflichtig sein, wenn diese Angriffe direkt unter Ausnutzung von Finanzdienstleistungen und unter Einschaltung des Instituts vorgenommen werden. Eine allgemeine Beratungs- oder Warnpflicht dem Kunden gegenüber entsteht daraus jedoch nicht. Es ginge, wie noch zu zeigen sein wird, zu weit, den Kunden vor jedwedem Kriminalitätsrisiko oder Verlustrisiken aus Hoch-Risiko-Geschäften schützen zu wollen.

Ein kurzer Rückblick auf den Regelungszusammenhang vor 2011 soll helfen, die seinerzeitige Erweiterung des Aufgabenspektrums besser einzuordnen und die weitere Entwicklung im Rahmen der Gesetzgebung zur Bewältigung der Finanzkrise im Gesamtzusammenhang zu sehen:

1.2 Die bisherige Regelung: § 25c KWG (alt)

Im Kreditwesengesetz war die Pflicht der Institute, „interne Sicherungsmaßnahmen“ zu schaffen, seit 2008 wie folgt geregelt:

> *Institute haben unbeschadet der in § 25a Abs. 1 dieses Gesetzes und der in § 9 Abs. 1 und 2 des GWG aufgeführten Pflichten im Rahmen ihrer ordnungsgemäßen Geschäftsorganisation und des angemessenen Risikomanagements zur Verhinderung von betrügerischen Handlungen zu ihren Lasten interne Grundsätze und angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen und zu aktualisieren und Kontrollen durchzuführen.*

Durch das Wort „unbeschadet“ wurde klargestellt, dass die internen Sicherungsmaßnahmen zur „Betrugsabwehr“, hier „Verhinderung von betrügerischen Handlungen zu ihren Lasten“ genannt, gleichrangig mit den Maßnahmen des Risikomanagements (§ 25a KWG, MaRisk) und mit der allgemeinen Compliance, der bankaufsichtsrechtlichen (Wertpapier-) Compliance (WpHG, MaComp) und der Geldwäschebekämpfung (GwG) einhergehen. Damit war die lediglich beiläufige Betrachtung des Themas Betrug und seine Behandlung als unselbstständiger Anhang der Geldwäschebekämpfung endgültig passé.

Der Frage, welche internen Sicherungsmaßnahmen nunmehr im Einzelfall zu treffen sind, welcher Umfang an Sicherung und Kontrolle für welches Institut angemessen ist und wie bei ihrer Implementierung vorgegangen werden kann, werden wir uns im Teil C dieses Buches ausführlich widmen. Vorab nur so viel: Was „angemessen“ ist, hat die BaFin in ihrem Rundschreiben 8/2005 (GW) unter Bezugnahme auf den damaligen § 25a Abs. 1 Satz 3 Nr. 6 KWG wie folgt umschrieben:

> *„Angemessen sind dabei solche Maßnahmen und Systeme, die der Risikosituation des einzelnen Instituts entsprechen und diese hinreichend abdecken. Die Sicherungssysteme haben sich insbesondere an der Größe, Organisation und Gefährdungssituation des einzelnen Instituts, insbesondere dessen Geschäfts- und Kundenstruktur auszurichten.“*

Und weiter heißt es:

> *„Was angemessen ist, beurteilt sich – wie auch sonst im Rahmen der Schaffung von Risiko-Management-Systemen – auf der Grundlage der eigenen Gefährdungsanalyse des Instituts bezüglich der Risikostruktur der von dem Institut angebotenen Dienstleistungen. Die Systeme sind laufend neuen Erkenntnissen und Gefährdungslagen anzupassen.“*

Es geht also bei der Frage der Angemessenheit um den institutsbezogenen, individuellen und risikogerechten Zuschnitt der Maßnahmen durch geeignete Prozesse, Organisationsrichtlinien und Dokumentation sowie eine Sicherstellung der erforderlichen technisch-organisatorischen Ausstattung, kurz: die Verfolgung des risikobasierten Ansatzes.

Der gesetzgeberische Wille, der in § 25c KWG (alt) zum Ausdruck gekommen war, umfasste die Verpflichtung zur Betrugsprävention durch Gestaltung der Geschäftsorganisation, zur Schaffung kundenbezogener Sicherungssysteme, zur Schaffung interner Grundsätze und eines entsprechenden Kontrollumfeldes.

Keine Erwähnung fand die Pflicht zur Sachverhaltsermittlung im Einzelfall. Das sind aber zweierlei Gegenstände: Das Gesetz verlangt zum einen generelle, vorbeugende Maßnahmen, also Prävention. Zum anderen soll auf Einzelfälle angemessen reagiert werden, was eine repressive (Strafverfolgung durch Strafanzeige) Vorgehensweise voraussetzt. Im Zusammenhang institutsinterner Vorgehensweise nennen wir den verfolgenden Teil hier „responsives" Handeln, da repressives Vorgehen ausschließlich staatlichen Organen vorbehalten ist und die richtige „Response" auch in der Geltendmachung zivilrechtlicher Ansprüche (Schadenersatz) oder in arbeitsrechtlichen Maßnahmen liegen kann. Zudem verlangt das Gesetz, wie noch zu zeigen sein wird, nur die Prüfung der Erstattung einer Strafanzeige. Ob tatsächlich ein Sachverhalt bei den Ermittlungsbehörden angezeigt wird, unterliegt hingegen einem breiten Ermessensspielraum.

„Responsives" Handeln bedeutet also, dass der entdeckte Vorfall eine Reaktion erfährt und nicht unbeantwortet bleibt. Welche Antwort in der jeweiligen Situation angemessen ist, wird anhand der Ergebnisse der Untersuchungen entschieden.

1.3 Prävention und Ermittlung

Präventives und responsives Vorgehen unterscheiden sich in Technik, Mitteln und Zielen des Herangehens ganz grundsätzlich. Während Prävention auf die Erkennung und Verhinderung zukünftiger, noch nicht verwirklichter Risiken und Gefahren ausgerichtet ist, verfolgt die Ermittlung das grundsätzliche Ziel, bereits begangene Taten aufzuklären und die erforderlichen Beweismittel bereitzustellen, um den Täter zur Verantwortung ziehen zu können.

Der entdeckten Tat eine Folge zu geben, das Geschehene mithin nicht einfach nur reaktionslos zur Kenntnis zu nehmen, kann zwar auch wieder präventive Wirkung entfalten, da potenzielle zukünftige Täter abgeschreckt werden und sich ein anderes Angriffsziel suchen. Diese generalpräventiven Wirkungen sind aber nicht der wesentliche oder ausschließliche Zweck responsiven Handelns. Im Gesetzestext des § 25h KWG geht die Differenzierung zwischen Prävention und Tataufklärung leider fast vollständig verloren, wodurch insbesondere in methodischen Fragen eine Vielzahl von Friktionen und Verwerfungen geschaffen werden. Hauptgrund mag die Unentschlossenheit des Gesetzgebers sein, wie die Verpflichteten mit aufgeklärten Taten umzugehen haben. Weder kommt im Gesetz ein „Null-Toleranz-Prinzip“ zur Anwendung, das eine Pflicht zur Erstattung von Strafanzeigen vorausgesetzt hätte, noch werden dem Anwender klare Vorgaben gemacht, wie eine Untersuchung angemessen durchzuführen sei und welche Reaktionsmechanismen welchem Ergebnis angemessen sind.

Die Methode der Wahl zur Tataufklärung ist die Ermittlung, die das Gesetz jetzt „Untersuchung“ des Sachverhalts nennt und bei Vorliegen bestimmter Voraussetzungen zur Pflicht macht. Ist sie abgeschossen, können die vorliegenden Indizien und Beweise bewertet und auf ihre Verwertbarkeit im zivilrechtlichen, arbeitsrechtlichen oder strafrechtlichen Verfahren begutachtet werden, um anhand einer Prognose über die Erfolgsaussichten zu einer Entscheidung über die weitere responsive Vorgehensweise zu gelangen.

Interne Ermittlungen, ihre rechtlichen und methodischen Voraussetzungen und Möglichkeiten beschreiben wir im Teil D dieses Buches.

Davon zu unterscheiden sind aber die Präventionsmaßnahmen, die der Gesetzgeber als dem Risikomanagement zugehörig bezeichnet und die in ihrer Gesamtschau eine Systematik der weitgehenden Straftatenverhinderung ergeben und bewirken sollen. Prävention hat nicht nur gänzlich andere rechtliche Voraussetzungen, sie hat auch völlig verschiedene Methoden und setzt eine grundsätzlich andere Denkweise voraus als die Ermittlung.

Solch deutliche Differenzierung scheint dem Gesetzgeber in seiner kriminalpolitischen Konzeption und der damit einhergehenden „Bekämpfungs-Rhetorik" nicht wichtig zu sein. Der Begriff der „Bekämpfung" – sei es die Bekämpfung der organisierten Kriminalität, die Geldwäschebekämpfung, die Bekämpfung der Terrorismusfinanzierung, die Rauschgiftbekämpfung und nicht zuletzt die Kriminalitätsbekämpfung, hat die klare konzeptionelle Trennung zwischen Prävention und Ermittlungen so sehr überlagert, dass eine rechtliche und methodische Trennlinie kaum noch gezogen werden kann.

Auch dieses Buch kann sich der entsprechenden Rhetorik nicht entziehen und verwendet bisweilen den Begriff der Kriminalitätsbekämpfung, da er nun in den neuen gesetzlichen Formulierungen seinen Niederschlag gefunden hat. Wir werden aber versuchen, die jeweiligen Methoden der Kriminalprävention und der Ermittlung voneinander getrennt zu sehen. Der teilweise heftigen Kritik, gerade vonseiten der Strafrechtswissenschaft, die an den neueren kriminalpolitischen „Bekämpfungs"-Konzepten geübt wird, schließen wir uns aufgrund vielfältiger Erfahrungen in den letzten Jahren an. Fischer (Strafgesetzbuch und Nebengesetze, 57. Aufl., 2010) schreibt im Hinblick auf den Geldwäschetatbestand und die Geldwäschebekämpfung:

> *„Entgegen den martialischen Absichtserklärungen „funktioniert" der Tatbestand in der Wirklichkeit eher virtuell: (…) das Konzept hat sich als eklatant unwirksam erwiesen. (…) Eine Verminderung der sogenannten organisierten*

Kriminalität ist nicht eingetreten. Die Relation der Gesamtkosten des Konzepts zu diesen tatsächlichen Erfolgen ist katastrophal. Nach rationalen Maßstäben ist das Konzept gescheitert. (…)

Dem hinter der Geldwäschebekämpfung stehenden kriminalpolitischen Konzept erteilt Fischer eine klare Absage:

„Seine Legitimierung weist Züge der Irrationalität auf. Seine Versprechungen stützt es auf eine Dynamik ständiger Erweiterung; stets fehlt zum großen Erfolg noch eine letzte Ausweitung des Tatbestands oder der Ermittlungsmöglichkeiten."

Harsche Worte eines amtierenden Vorsitzenden Richters am Bundesgerichtshof, die nur widerspiegeln, wie die Praxis inzwischen kriminalpolitische Entwicklungen empfindet, die schon vor geraumer Zeit kritisiert worden sind (Herzog 1996, 1999 und 2003; ausführlich Scherp, in WM, 2003, S. 1254 mit vielen Nachweisen).

Mein Fazit aus dem Jahr 2003 – damals zur abermaligen Neuregelung der Geldwäschebekämpfung – hat nahezu unverändert auch bei der aktuell vorgenommenen Neuregelung der Kriminalitätsbekämpfung durch KWG-Institute Gültigkeit:

1. Der Staat versucht dem Phänomen mit einer unklaren Bekämpfungsstrategie beizukommen und kann sich nicht recht entscheiden, ob die Schwerpunkte in der Prävention oder in der Repression gesetzt werden sollen.

2. Der inkonsistenten Strategie folgt eine an vielen Stellen ebenso inkonsistente Gesetzgebung nach, die das Verfassungsgebot der Verhältnismäßigkeit zuweilen außer Acht lässt.

3. Die Erfüllung der staatlichen Primäraufgaben – Prävention und/oder Repression – lässt in den hierzu verpflichteten Behördenapparaten an einigen Stellen zu wünschen übrig.

4. Die Indienstnahme von Privaten zu dieser Aufgabenerfüllung – hier der gesamten Kreditwirtschaft – hat einen Grenzwert erreicht, der eine weitere Ausweitung jedenfalls nicht mehr verhältnismäßig erscheinen lässt.

Über diese Aktualität kann ich mich indes kaum freuen, denn entgegen aller Mahnungen wird die „Kampfzone“ ständig ausgeweitet.

So weit, so gut, wird der Praktiker denken und sich die Frage stellen, wie er denn nun in der täglichen Praxis seines Instituts die Umsetzung der neuen Anforderungen bewältigen kann.

In die Kriminalitätsbekämpfung des KWG ist die Verdachtsmeldepflicht aus der Geldwäschebekämpfung nicht übernommen worden. Dafür trifft die Institute aber eine Untersuchungspflicht im Hinblick auf eine Vielzahl von Sachverhalten, die auf „sonstigen strafbaren Handlungen“ beruhen könnten. Die Übertragung originär staatlicher Aufgaben auf Private, also die Institute, ist so weit fortgeschritten, dass auch Sachverhalte zu dokumentieren sind, die zwar untersucht wurden, jedoch nicht zu einer Verdachtsmeldung oder Strafanzeige geführt haben. Darauf wird sogleich vertieft einzugehen sein. Auch in die Organisationshoheit der Institute wird tief eingegriffen: Die Bekämpfung der sonstigen Straftaten ist organisatorisch und funktional beim Geldwäschebeauftragten anzusiedeln, soweit die BaFin nicht im Hinblick auf vorzutragende wichtige Gründe eine Ausnahmeregelung für das einzelne Institut erlässt.

Begründet wird dies alles mit der Systematik des Risikomanagements, das es erfordere, die vom Gesetzgeber nur vage beschriebenen Risiken zu erkennen, zu managen und zu beherrschen. Die strafrechtsorientierte Bekämpfungsrhetorik wird so durch eine aufsichtsorientierte Risikorhetorik ergänzt. Die Entscheidung, welche Vorgänge tatsächlich den Verdacht einer Straftat recht-

fertigen und was zu melden ist, wird damit faktisch wieder den Instituten überantwortet. An der weiteren Unbestimmtheit der Kriterien, die dieser Entscheidung zugrunde zu legen sind, hat sich seit der Vorauflage nichts geändert.

Den Praktiker, an den dieses Buch sich richtet, braucht das alles nur am Rande zu interessieren. Er hat die gesetzlichen Vorgaben umzusetzen und im eigenen Institut so zu implementieren, dass die Maßnahmen den gestrengen Blicken des Wirtschaftsprüfers und der BaFin standhalten. Die aufsichtsrechtliche Sichtweise wird ihm dabei durch die Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft (DK – Hinweise) zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen" vermittelt, die die BaFin mit Rundschreiben 1/2012 (GW) zu ihrer Verwaltungspraxis erklärt hat (hier berücksichtigt: Stand 1. Februar 2014).

Weitere Erkenntnisse ergeben sich aus den Ende 2012 ebenfalls neu gefassten MaRisk, die in AT 4.4.2 Anforderungen an die Ausgestaltung der Compliance-Funktion im Institut formulieren, die nach BaFin-Auffassung ausdrücklich den Organisationsbereich des § 25h KWG und andere Compliance-Funktionen mit umfassen sollen.

1.4 Betrügerische Handlungen, Fraud und sonstige strafbare Handlungen

Die frühere Regelung hatte zum Gegenstand, betrügerische Handlungen zulasten des Instituts zu verhindern. Der Begriff der betrügerischen Handlungen war und ist nicht klar umrissen. Fest steht nur, dass er nicht auf die Straftatbestände des Betruges (§ 263 StGB) und der betrugsähnlichen Delikte (§§ 263a bis 265b StGB) beschränkt war, sondern auch die Untreue (§ 266 StGB) und weitere wirtschaftskriminelle Handlungen erfasste. Die Definition der Wirtschaftskriminalität im Sinne des Gerichtsverfassungsgesetzes (§ 74c GVG) hingegen stellte auch keine sachliche Begrenzung des Begriffs der betrügerischen Handlungen dar. Geschuldet war diese definitorische Offenheit der Übersetzung von Begriffen wie Fraud und fraudulent activities aus internationalen Papieren, Vereinbarungen und Direktiven.

Im englischen und amerikanischen Sprachraum findet sich für die hier zu betrachtenden Taten der generelle Oberbegriff Fraud. Das Substantiv Fraud direkt mit „Betrug“ zu übersetzen, verbietet sich jedoch, weil sonst der Blick auf § 263 des deutschen Strafgesetzbuchs eingeengt werden könnte. Darüber hinaus ist die Begrifflichkeit im anglo-amerikanischen Rechtsraum wesentlich breiter angelegt, da es zum einen an ausformulierten Gesetzestatbeständen fehlt, zum anderen auch Handlungsweisen erfasst werden, die im deutschen Rechtssystem dem Zivilrecht (unerlaubte Handlungen, arglistige Täuschung) zugerechnet werden.

Diese Bandbreite versuchte die deutsche Übersetzung „betrügerische Handlungen“ abzudecken, indem einerseits Straftatbestände erfasst werden, die nicht ausschließlich dem 22. Abschnitt des Strafgesetzbuchs mit der Überschrift „Betrug und Untreue“ unterfallen und letztlich auch Verhaltensweisen erfasst werden, die strafrechtlich nicht relevant sind und keinen strafgesetzlichen Tatbestand erfüllen. Es konnte sich hierbei um Formen der zivilrechtlichen Schädigung (arglistige Täuschung, unerlaubte Handlung) handeln, aber auch um Verwaltungsunrecht, dessen Ahndung als Ordnungswidrigkeiten durch Bußgelder oder durch (bank-)aufsichtsrechtliche Maßnahmen erfolgen kann. Damit bestand aber zugleich die Gefahr der Uferlosigkeit und der begrifflichen Entgrenzung der „betrügerischen Handlungen“.

Der nunmehr verwendete Begriff der „sonstigen strafbaren Handlungen“ ist zum einen sehr viel weiter: Fast das gesamte Spektrum möglicher Straftaten, die gegen ein Institut begangen werden können, ist jetzt erfasst. Praktisch das gesamte Strafgesetzbuch und viele Nebengesetze kommen als Tathandlungen in Betracht. Andererseits gibt es Einschränkungen, weil die außerstrafrechtlichen Schädigungshandlungen zukünftig nicht mehr erfasst sind. Diese und alle anderen grundlegenden Änderungen wollen wir uns im Folgenden näher ansehen.

2. Die aktuelle Fassung von § 25h KWG

2.1 Der Gesetzestext: Überblick

Der jetzt gültige § 25h KWG fasst unter der Überschrift „Interne Sicherungsmaßnahmen" die Präventionsmaßnahmen gegen Geldwäsche, Terrorismusfinanzierung und zur Verhinderung sonstiger strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können, zusammen.

Wichtigster Punkt der Neuregelung im Jahr 2011 war die Verlagerung des Aufgabenfelds von der „Verhinderung betrügerischer Handlungen gegen das Institut" hin zur Einrichtung eines internen Sicherungssystems zur Verhinderung sämtlicher „strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können".

Die Neuregelung hat bewirkt, dass alle Präventionsmaßnahmen zum allgemeinen Risikomanagement der Institute gehören.

Zur Verhinderung von vermögensgefährdenden strafbaren Handlungen wird den betroffenen Instituten eine Ermittlungspflicht auferlegt, die alle Transaktionen und Geschäftsbeziehungen umfasst, die ungewöhnlich oder auffällig sind und die keinen offenkundigen wirtschaftlichen oder rechtlichen Hintergrund haben. Den Auswirkungen dieser Untersuchungspflicht, die eng an die ohnehin schon bestehenden Monitoring-Verpflichtungen des Geldwäschegesetzes angelehnt ist, wird im Teil D dieses Buches näher nachgegangen. Erstaunlich ist, dass sich im Gesetzentwurf und seiner Begründung (BR-Drs. 482/10, S. 55 ff. und BT-Drs. 17/3023) bei der Betrachtung der Alternativen, Folgen und Auswirkungen des Gesetzes keinerlei Bezugnahmen zu dieser gänzlich neuen Verpflichtung finden. In der Gesetzesbegründung heißt es dazu lapidar:

„Daraus folgt, dass die Verhinderung von strafbaren Handlungen – ebenso wie die speziell geregelte Verhinderung von Geldwäsche und Terrorismusfinanzierung – nur unter Berücksichtigung der hierdurch der Kreditwirtschaft drohenden Schäden im eigenen Interesse der Institute liegt und damit zur

ordnungsgemäßen Geschäftsorganisation und zum Risikomanagement eines Instituts gehört. … Erfasst sind nach dem Sinn und Zweck der Regelung alle strafbaren Handlungen, die beim einzelnen Institut ein operationelles Risiko einschließlich eines Rechtsrisikos oder auch ein Reputationsrisiko begründen können. Als ein operationelles Risiko bei Instituten ist nach § 269 Abs. 1 Solvabilitätsverordnung die Gefahr von Verlusten anzusehen, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten und sich auf die Vermögenssituation des Instituts auswirken können. Zusätzliche Tatbestandsvoraussetzung ist jedoch, dass diese strafbaren Handlungen zu einer Gefährdung des Vermögens des Instituts führen können."

Wir wollen uns in den folgenden Kapiteln näher ansehen, welche strafbaren Handlungen die genannten Risiken im Institut begründen können und wie der Begriff der strafbaren Handlungen auszulegen ist. Unklar bleibt in diesem Zusammenhang weiterhin der Umgang des Gesetzgebers mit Ordnungswidrigkeiten oder unerlaubten Handlungen, die zwar nicht den Charakter einer Straftat haben, aber dennoch große Schäden für das Institut herbeiführen können. Denn sowohl die institutsinterne Begehung von Ordnungswidrigkeiten wie auch gegen das Vermögen des Instituts gerichtete unerlaubte Handlungen sind im Sinne der zitierten Gesetzesbegründung als operationelle Risiken einzustufen und dürften nicht selten Auswirkungen auf die Reputation haben. Der Wortlaut des Gesetzes begrenzt den Aufgabeninhalt dennoch und ohne Auslegungsspielraum auf strafbare Handlungen. Im Ergebnis wird man daher davon ausgehen müssen, dass die Behandlung von Ordnungswidrigkeiten und ihren Folgen in der Verantwortung der MaRisk-Compliance-Funktion, nicht aber bei der zentralen Stelle im Sinne des § 25h Abs. 9 KWG liegt. Zivilrechtliche Schädigungshandlungen könnten ebenfalls dort, aber auch bei einer Rechtsabteilung oder anderen operativen Stellen im Institut behandelt werden.

Von besonderer Brisanz für die Organisation im Institut dürfte sein, dass Ordnungswidrigkeiten und Straftaten sich bei nahezu gleichem Sachverhalt

oft nur in Nuancen unterscheiden. Durch die Aufgliederung der Zuständigkeiten werden damit nicht nur unklare Schnittstellen und mögliche Zuständigkeitskonflikte geschaffen, sondern auch die Gefahr der Behinderung einer sachgerechten Sachverhaltsaufklärung heraufbeschworen.

Gerade in der frühen Phase einer Untersuchung, oft aber auch noch zum Zeitpunkt der Entscheidung, ob und wie gegen die Aktivitäten des Täters weiter vorgegangen werden soll, werden Rückschlüsse auf subjektive Einstellungen des Täters noch nicht vorliegen, sodass der Entscheider häufig zwischen Straftat und Ordnungswidrigkeit nicht recht unterscheiden kann. Wie damit – unter dem Gesichtspunkt der Untersuchungspflicht in § 25h KWG – umzugehen ist, wird noch zu erörtern sein.

Darüber hinaus ist von Bedeutung, dass der Gesetzgeber auf eine dem § 11 GwG nachgebildete Meldepflicht verzichtet hat und insoweit auf die allgemeine Möglichkeit zur Strafanzeige gemäß § 158 StPO verweist. Mit dem Fehlen der Meldepflicht entfällt zugleich die in § 13 GwG vorgesehene Freistellung von der Verantwortlichkeit, wenn die institutsinternen Ermittlungen in eine Strafanzeige wegen einer Wirtschaftsstraftat münden. Auch insoweit sind umfassende Erwägungen im Institut anzustellen und entsprechende Entscheidungsprozesse und -kompetenzen einzurichten. Bevor wir uns den Pflichtenkreis und die Maßnahmen im Einzelnen anschauen, ist jedoch ein Blick auf den Gesetzestext insgesamt erforderlich.

Im Hinblick auf die oben dargestellten häufigen Änderungen des Gesetzestextes haben wir auf einen Abdruck in der vorliegenden zweiten Auflage verzichtet. Dem Anwender und Leser wird angeraten, sich den jeweils aktuellen Gesetzestext aus dem Internet zu beschaffen und in relativ kurzen Abständen zu überprüfen, ob er noch im Besitz einer aktuellen Fassung ist. Gedruckte Textausgaben oder Gesetzeskommentare können hier schon lange keine hinreichende Sicherheit mehr bieten. Als nützliches und verlässliches Instrument hat sich die Website http://www.buzer.de/gesetze erwiesen, die gelegentlich

schneller neue Texte bereitstellt, als die über www.bafin.de verlinkte Seite des Bundesministeriums der Justiz und für Verbraucherschutz.

2.2 Definition „strafbare Handlungen“

Zunächst muss der Begriff der „sonstigen strafbaren Handlung“, die die gesetzlich umrissenen Pflichten auslöst, einer näheren Betrachtung unterzogen werden. Unter **strafbaren Handlungen** versteht man in der Strafrechtswissenschaft alle jene menschlichen Verhaltensweisen, die den (objektiven) Tatbestand eines Strafgesetzes erfüllen, ohne dass es auf das Vorliegen von Rechtswidrigkeit und Schuld ankäme. Der Begriff umfasst damit jene Tatbestände, die im Strafgesetzbuch und in den Nebengesetzen niedergelegt und mit **Kriminalstrafe** (Geldstrafe, Freiheitsstrafe) bedroht sind.

Nicht erfasst sind von § 25h KWG daher alle **Ordnungswidrigkeiten**, die gegenüber der Straftat ein Aliud darstellen und lediglich mit Geldbuße, der das sozialethische Unwerturteil der Strafe fehlen soll, bedroht sind. Ob diese Ausgrenzung der Ordnungswidrigkeiten angesichts der Höhe drohender Geldbußen, der Möglichkeiten der Gewinnabschöpfung (§ 17 Abs. 4 OWiG) und möglicher sonstiger verwaltungsrechtlicher Folgen im Zusammenhang mit der Risikovorsorge im Institut Sinn macht, muss bezweifelt werden. Der gesetzgeberische Wille, im Rahmen des allgemeinen Risikomanagements die Institute zu verpflichten, Vorkehrungen gegen ernst zu nehmende wirtschaftliche Risiken zu treffen, wird durch die Wahl des engen Begriffs „strafbare Handlungen“ teilweise verfehlt. Daran ändert auch der bereits zitierte Hinweis in der Gesetzesbegründung nichts, wonach alle strafbaren Handlungen erfasst sein sollen, „die beim einzelnen Institut ein operationelles Risiko einschließlich eines Restrisikos oder auch ein Reputationsrisiko begründen können“. Die von der Begehung von Ordnungswidrigkeiten ausgehenden operationellen Risiken können um ein Vielfaches größer sein, als der durch einzelne Straftaten entstehende Schaden. Bedenkt man, dass Ordnungswidrigkeiten auch durch alle Personen begangen werden können, die im Unternehmen Leitungsaufgaben haben (§ 30 Abs. 1 Nr. 5 OWiG) und ihren Aufsichts- und Kontrollpflichten fahrlässig nicht nachkommen (§ 130 OWiG), so wird deutlich,

dass die Verhängung einer Geldbuße gegen das Unternehmen (§ 30 OWiG) oder seine Organe und Beauftragten (§ 9 OWiG) wegen Verletzung der Aufsichtspflichten ein wesentlich höheres und realistischeres Risiko darstellt, als das Erleiden von Millionenverlusten eines Instituts durch Kapitalanlagebetrug oder strafrechtlich nachweisbare Untreuehandlungen von Geschäftsleitungsmitgliedern.

Man könnte nun als Praktiker argumentieren und die Zuständigkeit der entsprechenden Stelle über das „Pflichtprogramm" des Gesetzgebers hinaus ausdehnen, indem Ordnungswidrigkeiten, die zu einer Gefährdung des Vermögens des Instituts führen können, ebenfalls entsprechenden Untersuchungshandlungen zugeführt werden. Anzeige könnte das Institut im Rahmen des § 46 Abs. 2 OWiG, der die Strafprozessordnung sinngemäß für anwendbar erklärt, ebenfalls erstatten. Jedoch ist zu bedenken, dass die weiteren Vorschriften über den **Datenschutz**, die in § 25h KWG enthalten sind, für solche Untersuchungshandlungen in OWi-Sachen keine ausreichende Rechtsgrundlage darstellen dürften. Besonders deutlich wird dies in § 32 BDSG, der Untersuchungshandlungen unter Verwendung von Mitarbeiterdaten nur zulässt, soweit der Verdacht einer Straftat hinreichend dokumentiert ist. Führt das Institut also Untersuchungen im Hinblick auf einen Ordnungswidrigkeiten-Verdacht durch, so sind die sich aus dem Datenschutz ergebenden Beschränkungen zu beachten und die Erlaubnisklausel zur Datenverarbeitung in § 25h Abs. 2 KWG greift genauso wenig wie die Erlaubnis zur Informationsübermittlung an andere Betroffene in § 25h Abs. 3 KWG, sobald klar ist, dass es sich bei dem untersuchten Vorgang nicht um eine strafbare Handlung handelt.

Ebenfalls nicht erfasst vom Begriff der strafbaren Handlung sind eine Vielzahl von zivilrechtlich **unerlaubten Handlungen**, die zwar Verluste herbeiführen und Schadensersatzpflichten des Täters oder des Instituts gegenüber Dritten auslösen können, jedoch nicht unter den Tatbestand eines Strafgesetzes fallen. Die in der Begründung des Gesetzentwurfs versuchte Definition einer strafbaren Handlung „von außen" zeigt zwar die Absicht des Gesetzgebers, verfehlt jedoch angesichts des eindeutigen Wortlauts der Vorschrift ihren

Sinn: „Drohende Vermögensgefährdungen des Instituts basieren beispielsweise auf Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum, strafrechtlich relevanten Verstößen oder Umgehungen von Rechtsvorschriften durch einen Dritten (Kunde, Nicht-Kunde).“ Strafbare Handlungen „von innen“ beschreibt die Entwurfsbegründung wie folgt:

> *„Ein solcher Fall umfasst eine drohende Vermögensgefährdung des Instituts z. B. aufgrund von Handlungen mit betrügerischer Absicht, Veruntreuung von Eigentum, aufgrund eines strafrechtlich relevanten Verstoßes gegen oder unter Umgehung von Verwaltungs-, Rechts- oder internen Vorschriften, wenn mindestens eine institutsinterne Partei (Mitarbeiter, Organ) an der strafbaren Handlung beteiligt ist.“*

Die Benutzung des Begriffs „drohende Vermögensgefährdung“ erweist sich ebenfalls als sprachlich misslungen und rechtlich unscharf. Bei den meisten einschlägigen Tatbeständen muss der Schaden oder Vermögensnachteil zur Tatbestandsverwirklichung eingetreten sein. Ist er es nicht, liegt allenfalls Versuch vor, der jedoch nicht bei allen wirtschaftskriminellen Tatbeständen strafbar ist.

Für den Anwender im Institut machen diese Formulierungen die Arbeit nicht leichter. „Umgehungen von Rechtsvorschriften“ sind nun einmal nicht notwendigerweise Straftatbestände, schon gar nicht, wenn es sich um „interne Vorschriften“ des Instituts selbst handelt, können aber erhebliche wirtschaftliche Schäden sowie Rechts- und Reputationsrisiken auslösen. Nach dem Wortlaut des Gesetzes können, ja müssen diese Handlungen, wenn sie nicht den Tatbestand eines Strafgesetzes erfüllen, mithin außer Acht gelassen werden. Im Rahmen eines sinnvollen Risikomanagements macht das hingegen keinen Sinn.

Keine Stütze im Gesetz findet die in den Auslegungs- und Anwendungshinweisen der DK angesprochene Beschränkung auf „wesentliche“ Vermögensgefährdungen. Die Anwendung eines risikobasierten Ansatzes mag sich zwar auf