Strafbare Handlungen und Betrugsprävention – was für die Praxis wichtig ist

Nicht nur systemrelevante Banken, sondern gerade auch Genossenschaftsbanken mit ihrer gelebten Kundennähe und ihrem regionalen Filialnetz sind oft Ziel krimineller Energie. Der folgende Beitrag spiegelt unsere Erkenntnisse aus über 400 Auslagerungsmandaten und gibt praxisbezogen Hinweise zum wirksamen Risikomanagement.

Aufgrund der vielschichtigen mikro- und makroökonomischen Bedeutung wird häufig von der Systemrelevanz bestimmter Banken oder auch der Finanzbranche insgesamt gesprochen.

Angesichts dieser systemischen Bedeutung der Banken als Wohlstandsfaktor sind die gesetzlichen und regulatorischen Anforderungen für den Finanzsektor sehr hoch – insbesondere hinsichtlich der Vorkehrungen, die Banken treffen müssen, um sich vor strafbaren Handlungen zu ihren eigenen Lasten zu schützen.

Auch und gerade Genossenschaftsbanken mit ihrer gelebten Kundennähe und ihrem lokalen und regionalen Filialnetz sind Ziel krimineller Energie. Dies zeigen z. B. die jüngsten Anstiege von Geldautomatensprengungen.

Besondere Relevanz – besondere Anforderungen

Um nicht zu einem Risiko für das Gesamtsystem zu werden, müssen Kreditinstitute gem. § 25h Abs. 1 Kreditwesengesetz (KWG) über ein angemessenes Risikomanagement sowie über Verfahren und Grundsätze verfügen, um strafbare Handlungen abzuwenden, die zu einer Gefährdung ihres Vermögens führen können. Dafür haben sie angemessene geschäfts- und kundenbezogene Sicherungssysteme zu schaffen und zu aktualisieren sowie Kontrollen durchzuführen.

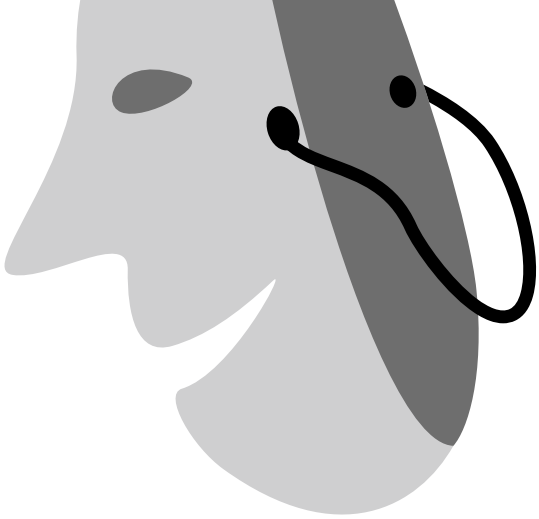
Der Begriff „strafbare Handlungen“, die zu einer (wesentlichen) Gefährdung des Vermögens des Instituts führen können, wurde vom Gesetzgeber bewusst nicht abschließend definiert.

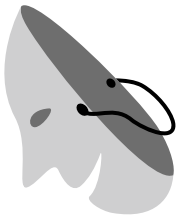
Eine Begriffsbestimmung wurde 2014 zwischen der Deutschen Kreditwirtschaft (DK), dem Bundesministerium der Finanzen und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in den damals geltenden Auslegungs- und Anwendungshinweisen vorgenommen.

Nach Sinn und Zweck der Gesetzesvorschrift umfasst der Begriff im Folgenden alle strafbaren Delikte, die zu einer Gefährdung des Vermögens des Instituts führen können. Dies kann durch vorsätzliche Handlungen externer und/oder interner Personen geschehen.

Zu den „strafbaren Handlungen“ im Sinne des § 25h Abs. 1 KWG zählen u. a.:

- Betrugs- und Untreuetatbestände
- Diebstahl
- Unterschlagung
- Raub und räuberische Erpressung
- Insolvenzstraftaten
- Ausspähen und Abfangen von Daten
- Identitätsdiebstahl





Zu einer wesentlichen Gefährdung der Vermögenslage zählen auch Reputationsschäden, die – ausgelöst z. B. durch negative Presseberichte oder (verfälschte) Nachrichten in den sozialen Medien – eine enorme Dynamik entfalten können.

Strafbare Handlung = Motivation + Möglichkeit

Die tatsächliche Ausführung hängt dabei nicht unbeträchtlich davon ab, welche (Gewinn-) Möglichkeiten – hier im Sinne von Erfolgsaussichten – das Ziel bzw. das potenzielle Opfer bietet.

Die Finanzbranche wird praktisch täglich mit strafbaren Handlungen konfrontiert. Das Augenmerk dieses Beitrags liegt – ausweislich der gesetzlichen Regelungen in § 25 KWG – auf den strafbaren Handlungen, die sich originär gegen die Bank richten. In diesen Fällen soll das betroffene Institut durch die strafbare Handlung bewusst und vorsätzlich geschädigt werden. Ein möglicher materieller oder immaterieller Schaden ginge zu Lasten der Bank.

Neben der Frage „Wer ist Ziel der strafbaren Handlung?“ ist im Rahmen der Präventionsmaßnahmen von wesentlicher Bedeutung, wer der Täter ist bzw. ob er oder sie außerhalb oder innerhalb des Unternehmens steht.

Zu den strafbaren Handlungen durch Dritte von außen, die sich gegen die Bank richten, zählen insbesondere:

- Einreichung gefälschter Überweisungsträger oder sonstiger Zahlungsaufforderungen per E-Mail oder Fax von vermeintlichen Kunden, Führungspersonen, Kollegen, Behörden etc.
- Einbruch/Diebstahl
- Konto-/Kartennutzung ohne Deckung
- Kreditbetrug
- Sachbeschädigung von Bankeigentum
- Sprengung/Aufbruch von Geldautomaten/Tresoren/Schließfächern

Strafbare Handlungen durch Dritte von innen (Mitarbeitende) sind häufig:

- Ungerechtfertigte Verfügungen von Konten
- Diebstahl (Wertgegenstände/Tresorinhalte)
- Eröffnung von „Fake-Konten“
- Gewährung von Darlehen ohne ersichtlichen Grund

Präventionsmaßnahmen

Je nachdem, ob strafbare Handlungen gegen eine Bank von internen oder externen Tätern ausgehen, werden verschiedene Abwehr- bzw. Sicherungsmaßnahmen in Kombination, aber mit unterschiedlichen Schwerpunkten eingesetzt.

Straftaten von außen begegnet ein Kreditinstitut insbesondere durch:

- Konsistente und intelligente Zugangsbeschränkungen für sensible Bereiche in der Bank
- Zuverlässige Alarm- und Videoüberwachungssysteme
- Moderne Schutzeinrichtungen für und Sichtprüfungen von Geldautomaten
- Gezielte Vorgaben und Regelungen in Form von Arbeitsanweisungen
- Stringente Kontrollprozesse hinsichtlich eingerichteter Systeme und eingereichter Dokumente
- Systemseitige Unterlegung des Vieraugenprinzips durch entsprechende (EDV-)Kompetenzregelungen
- Regelmäßige Schulung und Sensibilisierung der Mitarbeitenden

Um dolose Handlungen durch interne Täter zu verhindern, werden die meisten der oben aufgelisteten Maßnahmen ebenfalls – ggf. mit anderen Schwerpunkten – eingesetzt. Die besondere Schwierigkeit liegt dabei darin, dass Mitarbeitende die Sicherungssysteme kennen und unter Umständen auszuhebeln wissen.

Das bedeutet aber, dass neben „harten" Sicherungsmaßnahmen weiche Faktoren hinzutreten, die auf den Menschen bzw. die handelnde Person und ihr Verhalten gerichtet sind. Ganz allgemein lässt sich dieser Ansatz unter das Know-your-employee-/Know-your-colleague-Prinzip subsumieren. Dieses Prinzip setzt quasi vor der eigentlichen dolosen Handlung an und zielt auf die Zuverlässigkeit der Mitarbeitenden ab.

Dies beginnt praktisch schon vor der Einstellung von Mitarbeitenden. Die sorgfältige Prüfung eingereichter Bewerbungsunterlagen (Lebenslauf, Zeugnisse) sollte sich zu einem schlüssigen Bild einer Person zusammenfügen.

Die Einreichung und turnusmäßige Aktualisierung des polizeilichen Führungszeugnisses (z. B. nach drei Jahren) sollten im Bankalltag mittlerweile zum Standard gehören. Die Einrichtung eines internen Hinweisgebersystems ist seit 2. Juli 2023 nun ohnehin gesetzlich verpflichtend (hierzu auch unser entsprechender Fachbeitrag zum HinSchG in dieser PoC-Ausgabe).

Faktor Mensch

Von besonderer Bedeutung für die Verhinderung von dolosen Handlungen durch interne Täter ist allerdings das frühzeitige Erkennen von Warnsignalen. Im Einzelfall können diese als vorübergehend betrachtet werden, in regelmäßiger Kombination sollten sie jedoch unbedingt Beachtung und Würdigung finden und konkrete Maßnahmen auslösen.

Insbesondere folgende Typologien können Anzeichen für ein drohendes Fehlverhalten bzw. Gefahrenpotenzial sein.

- Bemerkenswerte Veränderungen im Wesen einer Person
- Grundlegende Veränderung im soziokulturellen Umfeld einer Person
- Häufige Nichteinhaltung von Vereinbarungen
- Vermeidung von (Urlaubs-)Abwesenheiten
- Kenntnis über finanzielle Probleme

Zahlen – Daten – Fakten

Wir haben in der DZ CompliancePartner GmbH als Mehrmandantendienstleister die im Vorjahr an uns gemeldeten Schadensfälle der Banken analysiert. Dabei wurden nur die Fälle berücksichtigt, die die jeweils bankspezifische Bagatellgrenze überschritten haben.

Die dolosen Handlungen lassen sich in folgender absteigender Reihenfolge sortieren.

- Überweisungsbetrügereien (inkl. Phishing)
- Automatensprengungen
- Einbruch
- Unterschlagung durch Mitarbeitende
- Sonstiges

An dieser Stelle besonders wichtig: Wird eine interne Straftat verhindert, wird nicht nur die Bank geschützt. Dem potenziellen Täter kann so auch Hilfe angeboten werden. Ein jähes Karriereende im Strafvollzug wäre nicht nur eine Belastung für den Täter, sondern auch für seine Familie und sein gesamtes persönliches Umfeld.

Unabhängig davon, ob strafbare Handlungen durch interne oder externe Täter verübt werden: Die eingerichteten Sicherungs- und Abwehrmaßnahmen greifen nur dann vollumfänglich, wenn sie durch alle Beteiligten gelebt und umgesetzt werden.

Insofern ist nicht nur die regelmäßige Sensibilisierung und Information der Mitarbeitenden von wesentlicher Bedeutung. Die Bank muss die entsprechende Compliance-Kultur über alle Hierarchiestufen vorleben.

Automatensprengungen

Wie bereits erwähnt, hat die Zahl der Automatensprengungen in den letzten Jahren stark zugenommen. Das Thema wird mittlerweile auch auf hoher politischer Ebene beobachtet und diskutiert. So gab es im Frühjahr dieses Jahres einen „Runden Tisch Geldautomatensprengungen" beim Bundesministerium des Innern. Ebenfalls im Frühjahr startete der BVR eine Umfrage unter den angeschlossenen Instituten. Die wichtigsten in diesen Gremien erarbeiteten Empfehlungen zur Verhinderung/Erschwerung von Automatensprengungen haben wir für Sie aufgelistet.

- Nachtverschluss bei SB-Foyers von 23:00 bis 06:00 Uhr
- Elektronische Überwachung durch qualifizierte Einbruchmeldetechnik
- Einsatz von Nebelsystemen (diese haben sich als besonders gute Schutzmaßnahme erwiesen)
- Einsatz von Einfärbe- und Klebesystemen
- Mechanische Schutzmaßnahmen
- Videoüberwachung
- Reduktion des Bargeldhöchstbestandes
- Standortwahl (Risikoanalyse der „Kommission Polizeiliche Kriminalprävention")

Technische Unterstützung durch Monitoring- und Fraud-Systeme

Die in bzw. für die Banken eingesetzten Monitoring- und Fraud-Systeme sind programmiert, um strafbare Handlungen – ob von intern oder extern – aufzudecken und zu verhindern. Diese technischen Unterstützungen sind flankierende Maßnahmen. Nicht jede Straftat kann im Vorfeld durch ein EDV-System oder Künstliche Intelligenz erkannt werden. Beispielhaft sei hier die nächtliche Automatensprengung genannt.

Dennoch runden Monitoring- und Fraud-Systeme das gesamte Maßnahmenpaket eines internen Kontrollsystems ab.

Fazit

Die Kreditwirtschaft hat in einer modernen Volkswirtschaft eine Schlüsselrolle. Daher wird häufig von der Systemrelevanz einzelner Banken bzw. der Branche an sich gesprochen.

Aufgrund dieser Sonderstellung sind die regulatorischen Anforderungen an die internen Sicherungsmaßnahmen in den Banken besonders hoch und auch gesetzlich verankert. Banken sind regelmäßig mit krimineller Energie von außen, aber auch von innen konfrontiert.

Basis für ein gut funktionierendes internes Kontrollsystem sind eine gelebte Compliance-Kultur und die schlüssige Kombination technischer und organisatorischer Sicherungsmaßnahmen. Nicht zuletzt haben die Sensibilisierung und Schulung der handelnden Personen besonderes Gewicht. ▬

Thomas Schröder
Abteilungsleiter Geldwäsche- und Betrugsprävention,
E-Mail: thomas.schroeder@dz-cp.de