Anti
Financial Crime
Alliance

AFCA

COVID-19-bezogene GW/TF-Risiken und Auswirkungen auf die Finanzkriminalität

AFCA - Public Private Partnership

Anti
Financial Crime
Alliance
AFCA

Inhaltsverzeichnis

I. Position der Financial Action Task Force (FATF) zu COVID-19

Anfang Mai veröffentlichte die FATF ein Positionspapier zum Umgang mit GW/TF-Risiken, die aus der COVID-19 Pandemie resultieren (Web-Link). Das Positionspapier zielt darauf ab, einen Rahmen im Umgang mit diesen neuen GW/TF Risiken zu setzen. Alle Beteiligten sollen ermutigt werden, die Hilfs- und Eindämmungsbemühungen von COVID-19 gemeinsam zu unterstützen und gleichzeitig wachsam im Hinblick auf gegenwärtige und aufkommende Risiken von Finanzkriminalität bleiben. Das Positionspapier konzentriert sich auf folgende Aspekte:

1. Entwicklung von GW/TF Risiken:

- Erhöhte GW-Bedrohung durch vermehrten Betrug, Cyberkriminalität als auch Auswirkungen auf andere Vortaten.
- Erschwerende Faktoren: Missbrauch von inländischen/internationalen Finanzhilfen u. Notfallfinanzierungen sowie erhöhte finanzielle Volatilität.

2. Aktuelle Auswirkungen von COVID-19 auf GW/TF-Regimes:

- Die COVID-19-Krise wirkt sich auf Schlüsselbereiche wie Aufsichtstätigkeit, Verdachtsmeldungen, FIU-Analysen, internationale Zusammenarbeit und Geschäftskontinuität des Privatsektors aus.

3. Mögliche Lösungsansätze zur Eindämmung der erhöhten GW/TF Risiken:

- Innerstaatliche Koordination zur Bewertung der Auswirkungen von COVID-19 im Kontext der GW/TF Bekämpfung.
- Verstärkte Kommunikation mit dem privaten Sektor und Überwachung der Auswirkungen von COVID-19.
- Verstehen der neuen Risiken und Entwicklung von passenden Maßnahmen.
- Ermutigung zur Ausschöpfung des risikobasierten Ansatzes.

Mit ähnlichem Inhalt hat auch die European Banking Authority (EBA) ein Papier veröffentlicht (Web-Link).

II. COVID-19 Faktoren, die Veränderungen in der Finanzkriminalität bewirken

Die COVID-19 Krise stellt die Finanzinstitute vor mehrere neue Herausforderungen und hat zu einem Anstieg der gesetzeswidrigen Aktivitäten geführt. Die bisher genutzten Mechanismen zur Erkennung von Finanzkriminalität müssen an das gegenwärtige Krisenumfeld angepasst werden. Kriminelle nutzen vor allem die aktuelle Situation der sozialen Distanzierung und Selbstisolierung aus; bisher angewandte kriminelle Methoden werden weiterentwickelt und/oder ersetzt.

Folgende Faktoren u. gesellschaftliche Entwicklungen wirken sich auf kriminelle Aktivitäten/Methoden aus:

- Geringere Mobilität innerhalb der EU und geringerer Zustrom von Menschen in die und aus der EU.
- Zunehmende Verbreitung der Telearbeit unter starker Nutzung digitaler Lösungen.
- Erhöhte Angst/Furcht innerhalb der Bevölkerung sowie wirtschaftlicher Abschwung können die Anfälligkeit für Ausbeutung und Betrug erhöhen.
- Hohe Nachfrage nach bestimmten Waren, Schutzkleidung und pharmazeutischen Produkten.
- Vermindertes Angebot bestimmter illegaler Güter infolge Grenzschließung und Eruierung von neuen Transportwegen.
- Einschränkungen des öffentlichen Lebens machen bestimmte kriminelle Aktivitäten weniger sichtbar und verlagern sie nach Hause oder ins Internet.
- Erhöhte Digitalisierung im Bankensektor durch stärkeren Anstieg der Online-Banking-Nutzung seitens der Kunden (Online-Banking) und bei der Kundenannahme/Identifizierung durch Institute.
- Mangelnde Vertrautheit mit Online-Plattformen/-Angeboten bei bestimmten Kundengruppen (z.B. aufgrund von Alter, Einkommen, Wohnort).
- Abwandern von Kunden zu nicht regulierten/unseriösen Anbietern.
- Vermehrte hohe Bargeldtransaktionen können Geldwäscheaktivitäten verschleiern.

III. Typische Covid-19 Delikte: Cyberkriminalität

Insbesondere die Einführung der Regeln zur sozialen Distanzierung und der „Lock down“ haben die Nachfrage nach Informationen und Angeboten über Online-Kanäle erhöht und zu einem deutlichen Anstieg der Sicherheitsrisiken geführt.

Anstieg der Cyberkriminalität:

- Eine deutliche Zunahme der Bedrohung durch Cyber-Vorfälle ist zu beobachten; insb. die Zahl der eingesetzten Malware-Techniken steigt an. E-Mails- und SMS-Phishing-Kampagnen mit COVID-19 Bezug zielen darauf ab, persönliche Zugangsdaten und andere sensible Daten zu sammeln, indem die Opfer verleitet werden, auf bestimmte Links zu klicken, die Informationen über Todesfälle, Heilung usw. versprechen. Die Malware-Zufuhr erfolgt hauptsächlich über SPAM-Kampagnen sowie über gefälschte oder nachgeahmte Webseiten.

- Die Erkenntnisse verdichten sich, dass der Einsatz von Betrugs- bzw. Erpressungssoftware eine besondere Bedrohung darstellt. Es gibt vermehrt Berichte über den Einsatz von Erpressungssoftware, die gegen Krankenhäuser und Gesundheitseinrichtungen gerichtet ist. „Business-Email Compromise (BEC) – Betrugsfälle“ nutzen die Schwachstellen in der Netzwerksicherheit von Unternehmen aus. Die Anzahl der registrierten Domains mit „Corona“- und „COVID“-Bezug nimmt stetig zu. Auch terroristische Vereinigungen versuchen, durch gezielte Spendenaufrufe mit COVID-19-Bezug, die Krise auszunutzen, um zusätzliche Gelder aufzubringen.

IV. Typische Covid-19 Delikte: Betrug

Kriminelle Akteure nutzen die COVID-19-Pandemie aus, um seit langem bekannte betrügerische Praktiken verstärkt anzuwenden (z. B. das Finanzagentenmodell). Daneben zeichnen sich bestimmte neue Muster ab.

- Insbesondere bei Betrugs- und Fälschungsdelikten, die bestimmte medizinische Güter, persönliche Schutzausrüstungen und pharmazeutische Produkte betreffen, ist ein deutlicher Anstieg zu verzeichnen.

- Die Muster im Kontext des Investitionsbetrugs, Vorauszahlungsbetrugs und Lieferbetrugs haben sich schnell an die aktuelle Krisensituation angepasst. Zudem ist vermehrt Investmentbetrug (Marktmanipulation) durch gezielte Falschmeldungen zu angeblichen COVID-19 Errungenschaften von Unternehmen mit geringer Marktkapitalisierung (microcap stocks) zu beobachten.

Die Betrüger verwenden raffinierte Social-Engineering-Techniken; sie nutzen das verstärkte Online-Engagement und die finanzielle Verwundbarkeit der Menschen aus, um verschiedene Betrügereien zu begehen:

- Anlagebetrug (Boiler-Room-Fraud).
- Romantikbetrug über Partnerschaftsportale (Scam).
- Kurierbetrug.
- Identitätsbetrug (Vortäuschung Behördenmitarbeiter oder Vorgesetzter (CEO) zu sein).
- Enkel-bzw. Neffen-Trick (Infizierter Angehöriger).
- Spendenbetrug (Täuschung über angebliche Sammlung mit COVID-19 Bezug).

V. GW-Hinweise zum Missbrauch der finanziellen Förderung

Aus deutscher Binnensicht konzentrieren sich die organisierten kriminellen Gruppen auf den Missbrauch der finanziellen Förderung, die die Regierung den kleinen und mittleren Unternehmen („Corona Soforthilfe“) gewährt. Das Ziel dieser Finanzmittel ist den KMU zu helfen, laufende Ausgaben für Mieten, Betriebskosten oder Löhne zu decken. Durch den Vorteil des dynamischen Antragsverfahrens und der verbesserten Malware-Techniken zum Diebstahl von Bankdaten versuchen die Kriminellen die Zahlungen schnell über das Banksystem umzuleiten. Kriminelle beantragen in betrügerischer Absicht die staatlichen Fördergelder. Dabei geben sie sich als legitime Unternehmen aus, die Unterstützung benötigen. Die folgenden Indikatoren können bei der Identifizierung von Konten, die im Rahmen der rechtwidrigen Beschaffung staatlicher finanziellen Unterstützung genutzt werden, hilfreich sein:

- Neu eröffnete Konten.
- Umsatzlose Konten mit deutlicher Zunahme des Umsatzes.
- Der Kunde erhält parallel Zahlungen von mehreren Finanzinstituten mit identischem Zweck.
- Der Kunde gehört eindeutig nicht zu den Personen oder Unternehmen, die unterstützungsberechtigt sind.
- Der Kunde beantragt eine Bevollmächtigung zu Gunsten Dritter.
- Der Kunde wickelt keine oder nur sehr wenige branchenspezifische Dienstleistungen über sein Konto ab.
- Gestiegener Umsatz seit März 2020.
- Bei eingehenden Gutschriften auf Konten:
  - die nicht als Geschäftskonten geführt werden.
  - Bei denen ein korrespondierendes Gewerbe zuvor abgemeldet wurde .
  - Bei denen abweichende Empfängernamen, als Begünstigte im Verwendungszweck genannt werden.
- Direkter Transfer von Subventionsgeldern im Anschluss nach deren Auszahlung auf verdächtige Konten.
- Häufige Zahlungsaufträge zum Transfer von Geldern zwischen verschiedenen Konten.
- Nachweis, dass mehrere Zahlungen, die anschließend zu Gunsten von Offshorekonten überwiesen werden, zunächst vom ursprünglichen Konto auf ein Sammelkonto überwiesen werden. (mit Hilfe von Finanzagenten).

VI. GW-Hinweise zum Missbrauch der Arbeitslosenhilfe

Vergleichbare Missbrauchsmuster zeigen sich im Rahmen der Arbeitslosenschutzmaßnahmen.

Eine gängige Methode, die von den Betrügern angewandt wird, ist das Klonen von Regierungs-Websites, mit dem Ziel, an Antragsdaten zu gelangen und das Geld für sich zu beanspruchen. Faktoren, die ein solches System anfällig für den Missbrauch durch Kriminelle machen, sind das dynamische Antragsverfahren und die mangelnde Erfahrung sowohl des öffentlichen als auch des privaten Sektors im Umgang mit solchen Verwaltungsverfahren in Zeiten einer Pandemie. Darüber hinaus ist der Zeitpunkt für die Wirksamkeit solcher Förderprogramme von entscheidender Bedeutung, d.h. Zeit für eine umfassende behördliche Prüfung ist nicht gegeben, Schnelligkeit hat den Vorrang. Die folgenden Indikatoren können bei der Identifizierung von Konten, die im Rahmen der rechtswidrigen Beschaffung staatlicher finanziellen Unterstützung genutzt werden, hilfreich sein:

- Neu eröffnete oder umsatzlose Konten.
- Überweisung der Arbeitslosengelder an Anbieter von Kryptowährungen, weitere Konten oder Barverfügungen.
- Unvereinbares Alter des Kontoinhabers.
- Kürzlich vorgenommene hochriskante Änderung von Schlüsselbezeichnungsdaten des Kontos, die auf einen Versuch der Umwidmung des Kontos hinweisen könnten.
- Der Kunde beantragt eine Bevollmächtigung zu Gunsten Dritter.
- Der Kunde ist zur Auszahlung der Subventionsgelder nicht berechtigt.

VII. GW-Hinweise zum Anlagebetrug

Ein weiterer Straftatbestand zur besonderen Aufmerksamkeit ist der Anlagebetrug. Charakteristische Opfertypen sind ältere Erwachsene mit beträchtlichen Ersparnissen oder Erwachsene in finanziellen Schwierigkeiten während der letzten Monate, die noch verfügbare Mittel verwenden, um in binäre Optionen, Gold oder Krypto-Währungen zu investieren. Sehr oft werden die überwiesenen Beträge in Tausenden von Euros auf die gleichen Konten gesendet. Kunden haben Bankberatern wiederholt mitgeteilt, dass ein Immobilienkauf ansteht, um die Vermögensverwaltung, Fondsanlagen, Bausparverträge oder Lebensversicherungen zu beenden. Die Zahlungsempfänger sind Drittanbieter von Zahlungsdienstleistungen, Krypto-Währungswechsel, bei denen die physische „Brieftasche“ dem Betrüger gehört. Der Missbrauch virtueller Vermögenswerte zum Zweck der Geldwäsche bzw. dem Verbergen inkriminierter Gelder ist ein ernstzunehmender Punkt, der während der Pandemiekrise zu berücksichtigen ist. Warnhinweise zur Identifizierung von Konten, über die solche betrügerische Aktivitäten erfolgen:

- Hohes Einlagenvolumen innerhalb eines kurzen Zeitraums.
- Große Mengen an Bargeld aus ungeklärten/unplausiblen/unbekannten Quellen.
- Gemeinsamer geographischer „Fußabdruck“ von Einlegern/Kontoinhaber.
- Transaktionen, die nicht mit dem Kundenprofil übereinstimmen.
- Bei „Goldbetrug“ zu Lasten des Kunden: Überweisung eines Betrags, der nicht dem Marktpreis des zu erwerbenden Goldes entspricht (Der Betrag liegt deutlich unter dem Marktpreis des Goldes).

VIII. Neue / aufkommende Risiken für Finanzkriminalität durch COVID-19

KMU werden als Werkzeug für Geldwäsche verwendet

- Wenn ein kleines oder mittelständisches Unternehmen (KMU) von einer Bank zu einer bedeutenden Zahlung aufgefordert wird, könnten Umstände eintreten, unter denen es gezwungen ist, Erlöse von einer Gruppe der organisierten Kriminalität anzunehmen, um die Zahlung zu finanzieren.
- Dies kann im Austausch gegen einen Eigentumsanteil an dem Unternehmen erfolgen, wodurch illegale Erlöse in den Finanz- und Wirtschaftskreislauf eingeschleust werden.
- Kriminelle, die Gesellschafter eines KMU sind und/oder dieses kontrollieren, könnten die Rückzahlung des Darlehens als Rechtfertigung für die Überweisung von Geldern illegaler Herkunft verwenden, die anderswo deponiert wurden.

Eine hohe Volatilität auf den Finanzmärkten erhöht das Risiko für Geldwäsche

- Insider Trading wird erleichtert. Personen könnten versuchen, Insiderinformationen auszunutzen oder den direkt mit COVID-19 und dem Pharmasektor verbundenen Markt zu manipulieren (z. B. durch Verbreitung falscher Informationen) und die Erlöse über die Finanzinstitute zu waschen.
- Der Wertverlust von bestimmten Anlageprodukten veranlasst die Anleger, diese zu verlagern oder sich von diesen komplett zu trennen, um die Verluste zu minimieren. Diskontierte Vermögenswerte beim Verkauf öffnen den Kriminellen die Tür für den Kauf oder die Refinanzierung solcher notleidenden Vermögenswerte mit Hilfe illegaler Gelder.

Ausnutzung des Bankensystems für GW-Aktivitäten

- Es besteht die Gefahr, dass Kriminelle NPOs und karitative Organisationen für damit verbundene Steuervorteile nutzen, um illegale Gelder zu waschen.
- Kriminelle können auch illegale Erlöse in das Finanzsystem einbringen, indem sie bestehende Kredite umschulden.
- Kriminelle versuchen vorübergehende Systemdefizite der Institute auszunutzen und Customer Due Diligence Anforderungen zu umgehen.

IX. Weitere Indizien zur Abgabe von Verdachtsmeldungen

Die Pflicht zur Erstattung einer Verdachtsmeldung richtet sich danach, ob der unrechtmäßigen Inanspruchnahme insbesondere ein gewerbs- oder bandenmäßiger Betrug zugrunde liegt. Da der einfache (Subventions-) Betrug keine Vortat zur Geldwäsche ist, wäre seitens des Verpflichteten zu prüfen, ob ein Alert ausreichende Indizien beinhaltet, die auf einen gewerbs- oder bandenmäßigen Betrug schließen lassen.

Hinweise insbesondere für einen gewerbsmäßigen Betrug im Umgang mit den Soforthilfen sind:

- Rückschlüsse auf das Vorliegen eines sog. Finanzagenten-Modells (z. B. weil die Soforthilfe bar verfügt oder weiter überwiesen wird, bspw. an einen Empfänger im Ausland, Money Service Business Provider oder Virtual Currrency Provider).

- Indizien für die Gründung von Scheinfirmen zur Erlangung unrechtmäßiger Zuwendungen oder Indizien für die konzertierte Beantragung von Fördermitteln durch mehr als zwei Personen (z. B. der gleichen Familie) zur Erlangung unrechtmäßiger Zuwendungen in einem größeren Umfang.

Da die Sofortmaßnahmen im Zusammenhang mit der Corona-Pandemie an sich nur eine einmalige Antragstellung und Auszahlung vorsehen, kann es an dem Tatbestandsmerkmal der (beabsichtigten) wiederholten Begehung und damit dem gewerbsmäßigen Betrug fehlen. Auffälligkeiten begründende Indizien können beispielsweise Soforthilfen sein, die von Sozialleistungsempfängern, Rentnern, Schülern, Studenten, Auszubildenden oder anderen Personen entgegengenommen werden, deren Konten ganz offensichtlich keine gewerblichen Umsätze aufweisen und die offenkundig keinen Anspruch auf die erhaltene Soforthilfe haben.