



Deutscher Factoring
Verband e.V.

Behrenstraße 73
10117 Berlin

DEUTSCHER
FACTORING
VERBAND E.V.

Bundesanstalt für
Finanzdienstleistungsaufsicht
Referat BA 54
Graurheindorfer Str. 108
53117 Bonn

Deutsche Bundesbank
Abteilung B 30
Postfach 10 06 02
60006 Frankfurt am Main

- per E-Mail an: Konsultation-13-20@bafin.de; B34_MaRisk-BAIT@bundesbank.de; Konsultation-14-20@bafin.de; B30_MaRisk@bundesbank.de -

Berlin, den 23.11.2020

Stellungnahme im Rahmen der Konsultationen 13/2020 (BA) und 14/2020 (BA) – BAIT- und MaRisk-Novellen

Geschäftszeichen Konsultation 13/2020: GIT 3-FR 1903-2019/0020

Sehr geehrter Herr Röseler,
sehr geehrter Herr Prof. Dr. Wuermeling,
geehrte Damen und Herren,

als maßgebliche Interessensvertretung der deutschen Factoring-Branche (Stand November 2020: 45 Mitglieder, Gesamtumsatz der Mitglieder in 2019: rund 275 Mrd. Euro, Marktanteil unserer Mitglieder nach neutralen Analysen: rund 98 Prozent des Umsatzvolumens der in Deutschland verbandlich organisierten Factoring-Unternehmen) möchten wir Ihnen heute unsere Stellungnahme zu den BaFin-Konsultationen 13/2020 (BA) und 14/2020 (BA) zu den Entwürfen der Neufassungen der BAIT und MaRisk zukommen lassen.

1. Anmerkungen zum Entwurf der MaRisk-Novelle

Ein **zentraler Bereich der Neuerungen in den MaRisk betrifft den Umgang mit NPL und Forbearance**: Institute mit einer Quote notleidender Kredite von 5% oder mehr sollen in den MaRisk künftig als Institute mit hohem NPL-Bestand besonderen Regelungen und Anforderungen unterliegen, die auf die EBA NPL Guidelines zurückzuführen sind. Zu diesen besonderen Regelungen und Anforderungen gehören u.a. AT 2.1. Tz. 1 (Definition von NPE), AT 4.2. Tz. 3 (Auswirkungen der Strategie für notleidende Risikopositionen auf das Kapital) und AT 4.1 Tz. 11 (Prozess zur Planung des zukünftigen Kapitalbedarfs).

Wir möchten in diesem Zusammenhang darauf hinweisen, dass die **EBA NPL Guidelines sich auf das NPE-Management von Kreditinstituten beziehen, mit Blick v.a. auf das traditionelle Kredit- und Darlehensgeschäft** konzipiert wurden und zudem Begrifflichkeiten nutzen bzw. auf Begrifflichkeiten Bezug nehmen, die aus der CRR stammen, bspw. „Risikoposition“ und die Definition von NPE nach dem aufsichtlichen Meldewesen infolge der CRR-Ausfalldetektion.

Ähnliches trifft letztlich auch auf die **neuen Regelungen zu Forbearance in BTO 1.3.2** zu, die **für das traditionelle Kreditgeschäft passen, jedoch nicht für das Factoring als Forderungskauf**, bei dem der Debitor eine oder mehrere Forderungen aus Lieferung und Leistung zu zahlen hat, nicht jedoch ein Darlehen o.ä. zurückzuzahlen oder zu tilgen hat. Auch das in BTO 1.3.2, Tz. 1 genannte Ziel von Forbearance-Maßnahmen, einen „tragfähigen, nicht notleidenden Rückzahlungsstatus“ zu erreichen, passt grundsätzlich nicht zum Factoring als Forderungskauf, bei dem grundsätzlich keine Forbearance-Maßnahmen angewendet und zudem aufgrund der factoringspezifischen Dreieckskonstellation zwischen der Beziehung zum Factoringkunden und dem Forderungseinzug gegenüber dem Debitor unterschieden wird. Ebenso wenig passen die in BTO 1.3.2, Tz. 3 vorgesehenen Einstufungen von Risikopositionen als notleidende oder nicht notleidende (Forborne-)Risikopositionen nebst der dazugehörigen Einstufungskriterien zum Factoring; eine entsprechend vorgenommene „künstliche“ bzw. erzwungene Einordnung würde zu einer unzutreffenden Klassifizierung als NPE bzw. Forborne-Risikoposition und damit zu fälschlicherweise erhöhten Ausfallwahrscheinlichkeiten und negativen Bonitätsbeurteilungen führen.

Für Factoring bzw. Factoringanbieter (insbesondere Nicht-CRR-Kreditinstitute und Finanzdienstleistungsinstitute, die Factoring anbieten) sollten diese Vorgaben zu NPL und Forbearance somit nicht gelten, und dies sollte ausdrücklich klargestellt werden, um hier Rechtssicherheit für alle Marktteilnehmer zu schaffen. Für auf Factoring spezialisierte Finanzdienstleistungsinstitute sind insofern auch die entsprechende Ausnahme- und Sonderregelungen in § 2 Abs. 7a KWG (einschließlich der Ausnahmen von der CRR) sowie im Risikotragfähigkeitsleitfaden von BaFin und Bundesbank vom Mai 2018 (siehe dort Fußnote 1: *„Die in diesem Leitfaden niedergelegten Kriterien und Grundsätze knüpfen an AT 4.1 MaRisk an und sind ausdrücklich auf Kreditinstitute zugeschnitten. Da Finanzdienstleistungsinstitute gemäß AT 2.1 Tz. 2 die Anforderungen der MaRisk nur insofern zu beachten haben, wie dies vor dem Hintergrund der Institutsgröße sowie von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten zur Einhaltung der gesetzlichen Pflichten aus § 25a KWG geboten erscheint, ist eine Übertragbarkeit der Grundsätze und Kriterien aus diesem Leitfaden auf Finanzdienstleistungsinstitute nicht ohne weiteres möglich und geboten.“*) zu beachten, die ebenfalls für eine solche Ausnahme sprechen.

Sofern entgegen unserer v.g. Auffassung die neuen Forbearance-Regelungen auch auf bspw. CRR-Kreditinstitute, die Factoring anbieten, anwendbar sein sollten, plädieren wir zumindest für eine **factoringspezifische Klarstellung**, dass bei der **Bestimmung von „forborne exposures“ nach BTO 1.3.2, Tz. 3** auf die Einzelrechnungs/-forderungsebene abzustellen ist und nicht auf sämtliche Forderungen gegen einen Debitor – insofern ist nämlich zu bedenken, dass die im Factoring angekauften Forderungen gegen einen Debitor aus grundsätzlich separaten Lieferungen und Leistungen resultieren, während z.B. die Zahlung von Darlehensraten im klassischen Kreditgeschäft aus einem Darlehensvertrag resultieren und somit mit einander verknüpft sind, gerade auch im Hinblick auf Zugeständnisse zugunsten des Kreditnehmers im Sinne der neuen Forbearance-Regelungen.

Der neu eingefügten **Erläuterung zur Risikotragfähigkeit nach AT 4.1, Rz. 1** zufolge können auch mehrere Risiken, die jeweils einzeln betrachtet unwesentlich sind, zusammengefasst als wesentlich einzustufen und dementsprechend angemessen im Rahmen der Risikotragfähigkeit zu berücksichtigen sein. Hierbei sollte **im Sinne der Proportionalität und einer Aufsicht mit Augenmaß** gerade bei nicht systemrelevanten Instituten **durch eine entsprechend klarstellende Ergänzung sichergestellt werden, dass nicht alle unwesentlichen „Kleinrisiken“ mit unverhältnismäßig hohem Aufwand dauerhaft zu steuern sind.**

Im Hinblick auf den **neuen Passus in den Erläuterungen zu AT 4.3.2, Tz. 1** plädieren wir für eine **Klarstellung, dass sich Tz. 1 nicht auch auf Sicherheiten bezieht**, wie durch die neu eingefügte Erläuterung suggeriert wird.

Weitere grundlegende und umfassende Änderungen der MaRisk sind in AT 9 bzw. in Bezug auf Auslagerungen geplant. Hierbei fällt insbesondere auf, dass v.a. AT 9 künftig **nicht nur Regelungen für wesentliche Auslagerungen, sondern z.T. für alle Auslagerungen enthalten soll**, was auf entsprechende Regelungen der durch die MaRisk-Novelle umzusetzenden EBA Outsourcing Guidelines zurückzuführen ist. Es wäre in diesem Zusammenhang **zu begrüßen, wenn sich diese Differenzierung zwischen wesentlichen Auslagerungen, nicht wesentlichen Auslagerungen und allen Auslagerungen (also wesentlichen und unwesentlichen Auslagerungen insgesamt) auch sprachlich durchgehend in den Anforderungen der MaRisk wiederfinden ließe**. Auch die EBA Outsourcing Guidelines differenzieren nur zwischen der Auslagerung „wesentlicher und kritischer Funktionen“ und solchen, die diese Kriterien nicht erfüllen (vgl. Rz. 12 der EBA Outsourcing Guidelines). Formulierungen wie in AT 4.2 (Erläuterung: „Im Falle umfangreicher Auslagerungen...“), AT 4.4.1 (Erläuterungen zu Key Performance Indicators bei NPE-bezogenen Risiken: „e) Sonstiges (... oder Auslagerungsaktivitäten)“) bzw. AT 9, Rz. 2 (Erläuterung: „Bei Auslagerungen von erheblicher Tragweite...“) sind in dieser Hinsicht leider wenig hilfreich.

Zudem sehen wir **Erläuterungsbedarf im Hinblick auf sowohl Begriff als auch Ziele der „Szenarioanalyse“ in AT 9, Tz. 2**, da unklar ist, ob insoweit die entsprechende Erläuterung zu Stresstests in AT 4.3.3, Tz. 1 auch hier zutreffend ist.

Im Hinblick auf die **Erläuterung zu AT 9, Tz. 7** ist anzumerken, dass durch die **Einbeziehung möglicher zukünftiger wesentlicher Auslagerungen unter die Anforderungen an schriftliche Auslagerungsverträge** die Prüfrechte nach AT 9, Tz. 7 lit. h und i **faktisch von vornherein in allen Auslagerungsverträgen vereinbart werden müssen**, auch in Verträgen zu unwesentlichen Auslagerungen – dies trägt zu einer **weiteren „Verwischung“ der Abgrenzung von wesentlichen und nicht wesentlichen Auslagerungen** bei und ist als nicht im Sinne einer proportionalen Ausgestaltung der MaRisk **abzulehnen**.

Ebenso plädieren wir für eine Umformulierung der **Erläuterungen zu AT 9, Tz. 10 und 12**: Den Revisionsbeauftragten bzw. Zentralen Auslagerungsbeauftragten unmittelbar der Geschäftsleitung zu unterstellen dürfte wenig praktikabel sein, da diese in der Regel innerhalb der Compliance-Organisationseinheit angesiedelt sind; daher wäre die **klarstellende Formulierung „Der Revisionsbeauftragte/Zentrale Auslagerungsbeauftragte hat einer Organisationseinheit anzugehören, die der Geschäftsleitung unmittelbar unterstellt ist.“** In beiden Fällen vorzuziehen.

In diesem Zusammenhang möchten wir zudem darauf hinweisen, dass die **Ausweitung der Organisationsrichtlinien auch auf Regelungen zu Verfahrensweisen bei allen Auslagerungen** aufgrund der Streichung des Wortes „wesentlichen“ in AT 5, Tz. 3 lit. f gerade bei kleineren Instituten, die tendenziell ein Mehr an Auslagerungen haben, zu einem erheblichen Mehraufwand insbesondere in der Dokumentation führen dürfte. Dies sollte vor dem Hintergrund einer proportionalen Ausgestaltung der MaRisk vermieden werden, weswegen wir die **Streichung dieser Änderung befürworten**.

In Bezug auf die geplanten Änderungen des Abschnitts zum Notfallmanagement in AT 7.3 möchten wir vor dem Hintergrund der proportionalen Ausgestaltung der MaRisk darauf hinweisen, dass **jährliche Aktualisierungen des Notfallkonzepts gerade kleinere Institute vor Herausforderungen stellen dürften**. Ein **institutsindividueller und risikoadäquater Zeitraum bzw. Zeitrahmen** wäre hier somit angebracht. Auch ist leider unklar, was in den Er-

läuterungen zu AT 7.3, Tz. 1 mit dem Begriff „potentielle Gefährdungen“ gemeint ist; eine entsprechende **Verdeutlichung** wäre hier zu **begrüßen**.

Der **Eindeutigkeit halber** wären zudem weitere **Klarstellungen** in den Erläuterungen zu BTO 1.2.2, Tz. 2 zu „endfälligen Krediten“ (hierunter sind keine einzelnen Forderungen aus dem Factoring zu verstehen) und in BTO 1.2.5, Tz. 2 im Hinblick auf die bei der Wertermittlung von Sicherheiten zu berücksichtigenden externen Verwertungskosten zu **begrüßen**.

Zudem halten wir die in BTO 1.2.4, Tz. 2 **neu vorgesehene Votierung auch seitens des Bereichs Markt im Factoring für wenig sinnvoll**- sofern es bei einer Intensivbetreuung um die Bereitstellung neuer Finanzierungsmittel (insbesondere im Rahmen des klassischen Kreditgeschäfts) geht, mag dies zutreffen, nicht jedoch im Factoring. Wir befürworten daher eine entsprechende **Klarstellung**.

Abschließend möchten wir Ihre Pläne **begrüßen, die finale Fassung der MaRisk-Novelle erst im ersten Quartal 2021 zu veröffentlichen**, da so unnötige Diskussionen über die Geltung der MaRisk-Novelle für die Jahresabschlussprüfung 2020 vermieden werden können, die bei einer Publikation noch vor Jahresende erfahrungsgemäß unvermeidbar gewesen wären.

2. Anmerkungen zum Entwurf der BAIT-Novelle

Die BAIT-Novelle enthält nicht nur **z.T. weitreichende Veränderungen und Verschärfungen, die insbesondere für kleinere Institute herausfordernd** sind, sondern auch Ergänzungen und Änderungen, die überwiegend der generellen Klarstellung dienen und somit zu begrüßen sind (z.B. Punkt 6.4 zu den Gründen für eine unverzügliche Deaktivierung/Löschung von Berechtigungen, Punkt 7.2 zu den organisatorischen Grundlagen für IT-Projekte oder Punkt 8.4 zur Wartung von IT-Systemen als Änderungen selbiger).

Vor dem Hintergrund der gerade für kleinere Institute herausfordernden Änderungen der BAIT plädieren wir dafür, **ähnlich wie in den MaRisk auch in den BAIT durchgehend deutlicher klarzustellen, dass auch in den BAIT der Grundsatz der „doppelten Proportionalität“ Geltung hat**, um gerade den kleineren Instituten die Erfüllung der Anforderungen zu ermöglichen. Hierzu gehört auch, dass insbesondere für technische, aber auch für organisatorische Neuerungen wie z.B. die Anforderung einer 2-Faktor-Authentifizierung nach Punkt 6.8 der BAIT risikogemessene Umsetzungsfristen vorgesehen werden, da eine Umsetzung direkt nach Inkrafttreten der BAIT-Novelle nicht realistisch erscheint.

In Bezug auf die **Punkte 3 und 4 zum Informationsrisikomanagement (IRM) und Informationssicherheitsmanagement (ISM)** ist zu beachten, dass die darin **aufgeführten Aufgaben in der Praxis z.T. anders verteilt** sind, so dass bspw. die Schutzbedarfsanalyse (vgl. Punkt 3.4 ff.) nicht beim IRM, sondern beim ISM liegt. Dies sollte **durch die BAIT weiterhin ermöglicht bzw. zumindest berücksichtigt** werden. Ebenso ist anzumerken, dass bspw. eine **funktionsmäßige Trennung von IRM und ISM oder von operativer IT und operativer IT-Sicherheit gerade in kleineren Instituten kaum bis gar nicht durchführbar** ist, weswegen entsprechende **Klarstellungen bspw. in Punkt 4.5 zu begrüßen** wären.

Der insgesamt **neu eingefügte Punkt 5 operative Informationssicherheit wurde weitgehend verschärft und dürfte viele (Factoring-)Institute vor Herausforderungen** stellen. In einem vorhergehenden Entwurf hieß dieser Abschnitt 'Operative IT-Sicherheit', aber nunmehr steht der Abschnitt unter dem **Titel 'Operative Informationssicherheit'**, obwohl sich die **folgenden Regelungen weiterhin auf die IT-Sicherheit beziehen**. Hier wäre eine **Änderung des**

Titels sinnvoll, denn die Informationssicherheit hat andere Bezüge als IT-Sicherheit, so dass eine **unbeabsichtigte semantische Erweiterung zu vermeiden** ist.

Unter **Punkt 5.3** heißt es zur Auswertung von Gefährdungen des Informationssicherheitsverbundes: „Spätere Auswertungen umfassen u. a. forensische Analysen“. Hier wäre es **für die Praxis hilfreicher von „geeigneten Analysen“ zu sprechen**, da bei größeren Datenmengen meist sowieso automatisierte IT-Systeme vorangestellt sind und eine „forensische Analyse“ mit Blick auf die Größenordnung vieler Factoringinstitute hier insofern zu weitgehend erscheint

In Bezug auf die **Kann-Vorschrift zu Security Operation Centers (SOCs) in Punkt 5.5** („Die zeitnahe Analyse und Reaktion kann eine ständig besetzte zentrale Stelle, z. B. in Form eines Security Operation Centers (SOC), erfordern.“) ist anzumerken, dass im Hinblick auf die Proportionalität und Größe vieler (Factoring-)Institute die Anforderung, dauerhaft (24/7) ein SOC bereitstellen zu müssen, zu weitgehend wäre, so dass diese Kann-Regelung im Sinne der Proportionalität **zu begrüßen** ist. **Ähnliche proportionale Auslegungen sollten im Bereich des Security Information and Event Management (SIEM) anwendbar** sein.

Im Rahmen der **Überprüfung der Sicherheit der IT-Systeme nach Punkt 5.6** werden beispielhaft **Penetrationstests** als eine in Frage kommende Überprüfungsart genannt. Hierzu ist anzumerken, dass **regelmäßige Penetrationstests für kleinere Unternehmen nicht leistbar** sind; dies sollte somit im Sinne der Proportionalität z.B. im Rahmen des Schutzbedarfs mitberücksichtigt werden können.

Ähnlich wie bei der v.g. Anmerkung zum Titel von Punkt 5 ist auch die **Umbenennung des Punkt 6 von „Benutzerberechtigungsmanagement“ in „Identitäts- und Rechtemanagement“** im Hinblick auf den allgemeinen Sprachgebrauch eher unglücklich.

Unter Punkt 6 und hier insbesondere unter dem abgeänderten **Punkt 6.3** ist zudem nunmehr davon die Rede, dass **Zugriffe „auch bei nicht personalisierten Aktivitäten jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zuzuordnen sein“ müssen** – auch wenn der Sinn und Zweck dieser Regelung durchaus einzu-leuchten vermag, so möchten wir darauf hinweisen, dass die **praktische Umsetzung dieser Anforderung keineswegs einfach ist, da entsprechende (Monitoring-)Systeme nicht für jede Applikation oder Schnittstelle bereitstehen dürften**. Diese praktische Hürde ist von den Instituten, die den BAIT unterfallen, kaum beeinfluss- oder behebbar.

Punkt 6.7 betrifft die **Protokollierung und angemessene Überwachung von Aktivitäten mit privilegierten Benutzer- und Zutrittsrechten**. Hierzu möchten wir erneut auf die **Sondersituation insbesondere kleinerer Institute mit entsprechend kleineren IT-Teams** hinweisen, in denen **umfassende wechselseitige Vertretungen schon rein praktisch erforderlich** sind, so dass diese **Protokollierungs- und Überwachungsprozesse u.U. alle Mitglieder des IT-Teams betreffen und daher als zu umfangreich bzw. nicht proportional anzusehen** wären.

Die Neuerungen in Punkt 8.6 weiten die Anforderungen zu „ungeplanten Abweichungen vom Regelbetrieb (Störungen)“ aus. Hier **plädieren wir schon aus Gründen der Proportionalität für eine nähere Präzisierung des Begriffs „Störung“**, um sicherzustellen, dass nur bestimmte Störungen, die u.a. auch eines gewissen Ausmaßes sind, diesen Prozessen unterfallen. Zudem ist dies **auch zur Abgrenzung gegenüber den Vorgaben in anderen Abschnitten der BAIT erforderlich**: Beispielfhaft werden in den unter Punkt 8.6 geforderten Standard-

vorgehensweisen Informationssicherheitsvorfälle angesprochen, die aber auch schon unter Punkt 5 im Abschnitt zur operativen Informationssicherheit Erwähnung finden und dort den Vorgaben zu sicherheitsrelevanten Ereignissen unterfallen.

Im Hinblick auf den ebenfalls komplett neu eingefügten **Punkt 10 zum IT-Notfallmanagement** möchten wir vor dem Hintergrund der proportionalen Ausgestaltung der BAIT darauf hinweisen, dass **jährliche IT-(Notfall-)Tests (vgl. Punkt 10.4) gerade kleinere Institute vor Herausforderungen stellen dürften**. Ein **institutsindividueller und risikoadäquater Zeitraum bzw. Zeitrahmen wäre hier somit angebracht**.

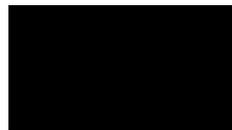
Abschließend möchten wir auch im Hinblick auf die BAIT-Novelle Ihre Pläne **begrüßen, die finale Fassung der BAIT-Novelle erst im ersten Quartal 2021 zu veröffentlichen**, da so unnötige Diskussionen über die Geltung der BAIT-Novelle für die Jahresabschlussprüfung 2020 vermieden werden können, die bei einer Publikation noch vor Jahresende erfahrungsgemäß unvermeidbar gewesen wären.

Für Rückfragen stehen wir Ihnen natürlich gerne zur Verfügung.

Mit freundlichen Grüßen



Dr. jur. Alexander M. Moseschus
Verbandsgeschäftsführer



Magdalena Wessel
Dezernentin Recht