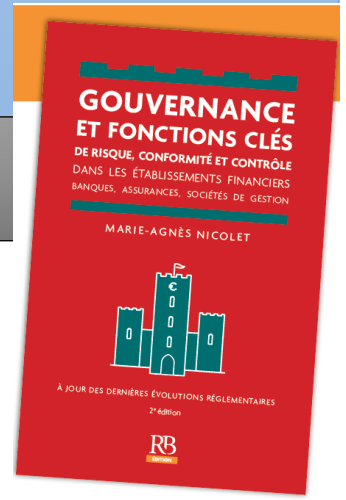
# Régulation financière : DSP2, Titrisation & Gouvernance

Conférence EIFR du 13 décembre 2018




**Marie-Agnès NICOLET**
**Regulation Partners**
Présidente fondatrice
35, Boulevard Berthier 75017 Paris
marieagnes.nicolet@regulationpartners.com
+33.6.58.84.77.40 / +33.1.46.22.65.34

# Sommaire

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Contexte réglementaire

| Procédure d'agrément des établissements de paiement et délais d'instruction | | | |
|---|---|---|---|
| Directive 2015/2366 | Ordonnance du 9 août 2017 | EBA/GL/2017/09 | Date d'application 13 janvier 2018 |

| Information clients et contrats | | | |
|---|---|---|---|
| Directive 2015/2366 DSP2 | Ordonnance du 9 Août 2017 | Arrêté du 31 Août 2017/contrat cadre de SP | Date d'application 13 Janvier 2018 |

| Mesures de sécurité des services de paiement –Gouvernance et risques opérationnels- | | |
|---|---|---|
| Directive 2015/2366 DSP2 | EBA/GL/2017/17 | Date d'application 13 Janvier 2018 |

| Détection des incidents et reporting des incidents majeurs et des fraudes liés aux opérations de paiement –Notification- | | | | |
|---|---|---|---|---|
| Directive 2015/2366 DSP2 | EBA/GL/2017/17 | EBA/GL/2017/10 | EBA/GL/2018/05 | Date d'application 13 Janvier 2018/ 1er janvier 2019 (Fraud reporting) |

| Mesures de sécurité des services de paiement –Authentification forte et normes communes et sécurisées de communication- | | | | |
|---|---|---|---|---|
| Directive 2015/2366 DSP2 | Règlement délégué (UE)2018/389 | Opinion de l'EBA sur la mise en place du SCA et CSC du 13 juin 2018 | Loi n°2018-700 du 3 août 2018 | Date d'application 14 Septembre 2019 et Test du système (API) le 14 Mars 2019 |

| Plan de continuité de l'activité (PUPA) | | |
|---|---|---|
| Directive 2015/2366 DSP2 | EBA/GL/2017/17 | Date d'application 13 Janvier 2018 |

# I. Suivi et reportings des fraudes liées aux services de paiement : les nouveautés liées à DSP 2

## Reporting relatif à la fraude

**L'article 96 de la directive 2015/2366 [DSP2] relatif à la notification des incidents, prévoit dans son (6) que les PSP doivent fournir aux autorités compétentes, au moins chaque année, des données statistiques relatives à la fraude liées au différent moyens de paiement.**

**L'EBA a publié une orientation portant application du (6) de l'article 96, « Guidelines on fraud reporting under Payment Services Directive PSD2 » du 18 juillet 2018 EBA/GL/2018/05.**

- **Ces orientations exigent que les prestataires de services de paiement fournissent à leurs autorités compétentes tous les (6) six mois un reporting en se basant sur le modèle fourni par l'EBA.**

**Le reporting doit comprendre toutes les transactions liées aux services de paiement et des fraudes sur ces services de paiement, notamment :**

- **Les opérations de paiement non autorisées qui résultent de la perte, du vol ou de l'utilisation frauduleuse des données de paiement sensibles ;**
- **La manipulation du payeur.**

Ces orientations sur les reporting en matière de fraude sont applicable à partir du 1er janvier 2019.

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Reporting relatif à la fraude : orientations de l'EBA relatives aux exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la DSP2

Aux fins de la déclaration des données statistiques relatives à la fraude, le prestataire de services de paiement devrait prendre en compte, pour chaque période de déclaration:

- ✓ Toute opération de paiement **non autorisée effectuée**, y compris à la suite de la perte, du vol ou de l'appropriation illicite de données de paiement sensibles ou d'un instrument de paiement, **qu'elle soit détectable ou non** par le payeur avant un paiement et résultant ou non d'une négligence grave du payeur ou exécutée en l'absence de consentement du payeur **(«opérations de paiement non autorisées»)** ;

- ✓ Toute opération de paiement effectuée **à la suite d'une manipulation du donneur d'ordre par le fraudeur**, ayant pour effet d'émettre un ordre de paiement ou de donner instruction de le faire au prestataire de services de paiement, de bonne foi, à un compte de paiement que le donneur d'ordre estime appartenir à un bénéficiaire légitime («manipulation du donneur d'ordre»).

Le prestataire de services de paiement (y compris, le cas échéant, l'émetteur de l'instrument de paiement) **ne devrait déclarer que les opérations de paiement qui ont été initiées et exécutées** (et acquises le cas échéant). Le prestataire de services de paiement ne devrait pas déclarer les données relatives aux opérations de paiement qui, n'ont pas été exécutées et n'ont pas entraîné de transfert de fonds.

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Reporting relatif à la fraude : orientations de l'EBA relatives aux exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la DSP2

Le prestataire de services de paiement **devrait communiquer les données tous les six mois.**

Le PSP bénéficiant d'une dérogation au titre de l'article 32 de la DSP2, ainsi que les établissements de monnaie électronique bénéficiant de la dérogation prévue par l'article 9 de la directive 2009/110/CE concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, **devraient déclarer l'ensemble des données demandées en utilisant des formulaires spécifiques** sur une base annuelle seulement, en répartissant avec les données sur deux périodes de six mois.

Le prestataire de services de paiement **devrait présenter les données** le concernant dans les délais fixés par les autorités compétentes respectives.

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Modèles de déclarations à l'intention des prestataires de services des paiement : Ventilation des données pour les virements

| | Libellé | Opérations de paiement | Opérations de paiement frauduleuses |
|---|---|---|---|
| 1 | **Virements** | **X** | **X** |
| 1.1 | Dont initiation par les prestataires de services d'initiation de paiement | X | X |
| 1.2 | Dont opérations initiées de manière non électronique | X | X |
| 1.3 | Dont initiation électronique | X | X |
| 1.3.1 | Dont opérations initiées via un canal de paiement à distance | X | X |
| 1.3.1.1 | **Dont opération avec authentification client forte** | X | X |
| | *dont virements frauduleux par type de fraude:* | | |
| 1.3.1.1.1 | Émission d'un ordre de paiement par le fraudeur | | X |
| 1.3.1.1.2 | Modification d'un ordre de paiement par le fraudeur | | X |
| 1.3.1.1.3 | Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement | | X |

*Source : orientations EBA concernant les exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la DSP2*

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Modèles de déclarations à l'intention des prestataires de services des paiement : Ventilation des données pour les virements

| | | | |
|---|---|---|---|
| **1.3.1.2** | **Dont opération avec authentification client non forte** | X | X |
| | *dont virements frauduleux par type de fraude:* | | |
| **1.3.1.2.1** | Émission d'un ordre de paiement par le fraudeur | | X |
| **1.3.1.2.2** | Modification d'un ordre de paiement par le fraudeur | | X |
| **1.3.1.2.3** | Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement | | X |
| | *dont ventilation par motif d'omission d'authentification client forte* | | |
| **1.3.2.1** | **Dont opérations avec authentification client forte** | X | X |
| | *dont virements frauduleux par type de fraude* | | |
| **1.3.2.1.1** | Émission d'un ordre de paiement par le fraudeur | | X |
| **1.3.2.1.2** | Modification d'un ordre de paiement par le fraudeur | | X |
| **1.3.2.1.3** | Manipulation du payeur par le fraudeur pour émettre un ordre de paiement | | X |
| **1.3.2.2** | **Dont opérations avec authentification client non forte** | X | X |
| | *dont virements frauduleux par type de fraude:* | | |
| **1.3.2.2.1** | Émission d'un ordre de paiement par le fraudeur | | X |
| **1.3.2.2.2** | Modification d'un ordre de paiement par le fraudeur | | X |
| **1.3.2.2.3** | Manipulation du payeur par le fraudeur ayant pour effet d'émettre un ordre de paiement | | X |
| | *dont ventilation par motif d'omission d'authentification client forte* | | |
| **1.3.2.2.4** | Paiement à soi-même (Art.15 RTS) | X | X |
| **1.3.2.2.5** | Bénéficiaire de confiance (Art.13 RTS) | X | X |
| **1.3.2.2.6** | Opération récurrente (Art.14 RTS) | X | X |
| **1.3.2.2.7** | Paiement sans contact de faible montant (article 11 RTS) | X | X |
| **1.3.2.2.8** | Automates de paiement des frais de transport et de parking (article 12 RTS) | X | X |

*Source : orientations EBA concernant les exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, paragraphe 6, de la DSP2*

# I. Suivi et reportings des fraudes liés aux services de paiement : les nouveautés liées à DSP 2

## Authentification forte du client et Normes communes et sécurisées de communication (API)

1/ Champ d'application et Obligations

2/ Définitions

3/ Dérogations

4/ Analyse des risques

5/ Normes communes et sécurisées de communication (Application Programming Interface)

# Authentification forte du client et Normes communes et sécurisées de communication (API)

## 1/ Champ d'application et obligations

**Champ d'application :**

Les services de paiement proposés par voie électronique devraient être sécurisés grâce à des technologies permettant de garantir une authentification sûre de l'utilisateur et de réduire, dans toute la mesure du possible, les risques de fraude.

Les exigences relatives à l'authentification forte du client qui devraient être appliquées chaque fois qu'un payeur :

- Accède à son compte de paiement en ligne ;
- Initie une opération de paiement électronique ; ou
- Exécute une action grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou de toute autre utilisation frauduleuse.

Dans les cas cités ci-dessus, les PSP devraient imposer un code d'authentification qui ne risque pas d'être falsifié, que ce soit dans son intégralité ou par la divulgation de l'un des éléments sur la base desquels il a été généré.

# Authentification forte du client et Normes communes et sécurisées de communication (API)

## 1/ Champ d'application et obligations

**Procédure d'authentification :** La procédure d'authentification devrait comprendre, en règle générale, des mécanismes de contrôle des opérations permettant de déceler les tentatives d'utiliser les données de sécurité personnalisées d'un utilisateur de services de paiement qui ont été perdues, volées ou détournées et devrait également garantir que l'utilisateur de services de paiement est l'utilisateur légitime et donne dès lors son consentement au transfert de fonds et à l'accès aux informations sur son compte au travers d'une utilisation normale des données de sécurité personnalisées.

**Exigences générales :** Pour garantir l'application de l'authentification forte du client, il est également nécessaire d'exiger des caractéristiques de sécurité adéquates pour les éléments d'authentification forte du client appartenant à la catégorie «connaissance», « possession » et « inhérence ».

*Les exigences relatives à l'authentification forte du client s'appliquent aux paiements initiés par le payeur que celui-ci soit une personne physique ou une personne morale.*

**Exigences particulières :** Les PSP devraient définir des exigences particulière pour les situations dans lesquelles le montant final n'est pas connu au moment où le payeur initie une opération de paiement électronique à distance, afin que l'authentification forte du client soit spécifique au montant maximal auquel le payeur a donné son consentement, conformément à la directive (UE) 2015/2366.

## 2/ Définition de l'authentification forte du client

**L'authentification forte du client :**

Une authentification reposant sur l'utilisation de **deux éléments** ou plus appartenant aux **catégories «connaissance», «possession» et «inhérence»** (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification.

1. **Connaissance** : quelque chose que seul l'utilisateur connaît (*comme un mot de passe, un code d'identification personnel, ou un « code PIN », etc.*)

2. **Possession** : quelque chose que seul l'utilisateur possède (*comme un «token », un téléphone mobile, une carte à micro-processeur ou « carte à puce » etc.*)

3. **Inhérence** : quelque chose qui est liée à la personne elle-même de l'utilisateur (*une caractéristique biométrique telle que l'empreinte digitale ou la voix par exemple*)

## 3/ Dérogations

Conformément à la directive (UE) 2015/2366 et au règlement délégué 2018/389, les dérogations au principe d'authentification forte du client ont été définies sur la base du niveau de risque, du montant, du caractère récurrent et du moyen utilisé pour exécuter l'opération de paiement.

### Dérogations applicables :

- Information sur le compte de paiement ;
- Paiement sans contact [montant ne dépassant pas 50€ et 150 € cumulés sur une période donnée, ou 5 opérations consécutives];
- Automates de paiement des frais de transport et de parking ;
- Opérations à faible valeur [montant ne dépassant pas 30€ et 100 € cumulés sur une période donnée, ou 5 opérations consécutives].

### Dérogations liées à l'analyse des risques :

- Bénéficiaires de confiance ;
- Opérations récurrentes ;
- Virements entre comptes détenus par la même personne physique ou morale ;
- Procédures et protocoles de paiement sécurisés utilisés par les entreprises.

**Applications des dérogations liées à l'authentification forte**

## 3/ Dérogations

Une opération de paiement électronique est considérée comme présentant un faible niveau de risque lorsque l'ensemble des conditions suivantes sont remplies :

- Le taux de fraude pour ce type d'opération, est équivalent ou inférieur aux taux de référence en matière de fraude mentionnés dans le tableau figurant sur le slide ci-après, pour les « paiements électroniques à distance liés à une carte » et les « virements électroniques à distance » respectivement ;
- Le montant de l'opération ne dépasse pas la valeur-seuil de dérogation correspondante mentionnée dans le tableau figurant sur le slide ci-après ;
- Le PSP n'a décelé aucun des éléments suivants à l'issue d'une analyse en temps réel des risques :
  - Des dépenses anormales ou un type de comportement anormal du payeur ;
  - Des informations inhabituelles concernant l'utilisation du dispositif ou logiciel du payeur à des fins d'accès ;
  - Des signes d'infection par un logiciel malveillant lors d'une session de la procédure d'authentification ;
  - Un scénario connu de fraude dans le cadre de la prestation de services de paiement ;
  - Une localisation anormale du payeur ;
  - Une localisation du bénéficiaire présentant des risques élevés.

## 3/ Dérogations

### Taux de fraude

La collecte de ces nouvelles données historiques sur les taux de fraude des opérations de paiement électronique contribuera également à un réexamen effectif par l'ABE des seuils applicables aux dérogations à l'authentification forte du client sur la base d'une analyse en temps réel des risques liés à l'opération.

**Calcul du taux de fraude :**

Le taux de fraude global lié à chaque type d'opération est calculé comme étant la valeur totale des opérations à distance non autorisées ou frauduleuses, dont les fonds ont été récupérés ou pas, divisée par la valeur totale de l'ensemble des opérations à distance pour le même type d'opération, authentifiées par une authentification forte du client ou exécutées au titre d'une dérogation, sur une base trimestrielle glissante (90 jours).

| Valeur-seuil de dérogations | Paiements électronique à distance liés à une carte | Virements électroniques à distance |
|---|---|---|
| 500 EUR | 0,01 | 0,005 |
| 250 EUR | 0,06 | 0,01 |
| 100 EUR | 0,13 | 0,015 |

**Suspension de la dérogation :**

Les prestataires de services de paiement cessent immédiatement de faire usage de la dérogation pour tout type d'opération de paiement à distance, lorsque le taux de fraude qu'ils contrôlent dépasse pendant deux trimestres consécutifs le taux de référence en matière de fraude applicable à cet instrument de paiement ou à ce type d'opération de paiement à l'intérieur d'une fourchette de 100 EUR à 500 EUR.

## 4/ Analyse des risques

Les PSP qui entendent exempter des opérations de paiement électronique à distance de l'authentification forte du client au motif qu'elles présentent un risque faible tiennent au moins compte des facteurs suivants liés aux risques :

- Les habitudes de dépenses antérieures de l'utilisateur individuel de services de paiement ;
- L'historique des opérations de paiement de chacun des utilisateurs de services de paiement du prestataire de services de paiement ;
- La localisation du payeur et du bénéficiaire au moment de l'opération de paiement dans les cas où le dispositif d'accès ou le logiciel est fourni par le prestataire de services de paiement ;
- L'identification de comportements de paiement anormaux de l'utilisateur de services de paiement par rapport à l'historique de ses opérations de paiement.

## 4/ Analyse des risques

### Mesures d'atténuation des risques :

Les prestataires de services de paiement qui font usage des dérogations prévus par le règlement font l'objet **au moins une fois par an d'un audit** portant sur la méthodologie, le modèle et les taux de fraude notifiés. L'auditeur qui réalise cet audit possède une expertise dans le domaine de la sécurité informatique et des paiements électroniques et est indépendant sur le plan opérationnel au sein du prestataire de services de paiement ou vis-à-vis de celui-ci. Au cours de la première année où il est fait usage des dérogations, et au moins tous les trois ans ensuite, ou plus fréquemment si l'autorité compétente le demande, cet audit est réalisé par un auditeur externe indépendant et qualifié.

# Authentification forte du client et Normes communes et sécurisées de communication (API)

## 5/ Normes communes et sécurisées de communication (Application Programming Interface) (1/3)

**Descriptions des exigences de l'interface API :**

Chaque prestataire de services de paiement gestionnaire de comptes qui gère des comptes de paiement accessibles en ligne **devrait proposer au moins une interface d'accès (API) permettant une communication sécurisée avec les prestataires de services d'information sur les comptes (PSIC), les prestataires de services d'initiation de paiement (PSIP) et les prestataires de services de paiement (PSP) qui émettent des instruments de paiement liés à une carte.**

Cette interface devrait permettre aux PSIC, aux PSIP et aux PSP qui émettent des instruments de paiement liés à une carte de s'identifier auprès du PSP gestionnaire du compte. Elle devrait également permettre aux PSIC et aux PSIP de s'appuyer sur les procédures d'authentification proposées par le prestataire de services de paiement gestionnaire du compte à l'utilisateur de services de paiement.

Pour garantir la neutralité du modèle commercial et des technologies, les PSP gestionnaires de comptes devraient être libres de décider s'ils proposent une interface dédiée à la communication avec les PSIC, les PSIP et les prestataires de services de paiement qui émettent des instruments de paiement liés à une carte ou s'ils autorisent, pour cette communication, le recours à l'interface servant à l'identification des utilisateurs de services de paiement des prestataires de services de paiement gestionnaires de comptes et à la communication avec ces utilisateurs.

## 5/ Normes communes et sécurisées de communication (Application Programming Interface) (2/3)

**Pour permettre aux PSIC, aux PSIP et aux PSP qui émettent des instruments de paiement liés à une carte de mettre au point leurs solutions techniques, les spécifications techniques de l'interface devraient être dûment consignées par écrit et publiées.**

**Par ailleurs, le PSP gestionnaire du compte devrait proposer un dispositif permettant aux prestataires de services de paiement de tester les solutions techniques au moins six mois avant la date d'application des présentes normes de réglementation ou, si le lancement a lieu après la date d'application des présentes normes, avant la date à laquelle l'interface sera lancée sur le marché.**

**Afin de garantir l'interopérabilité des différentes solutions de communication technologiques, l'interface devrait utiliser des normes de communication mises au point par des organisations européennes ou internationales de normalisation.**

## 5/ Normes communes et sécurisées de communication (Application Programming Interface) (3/3)

### Modification de l'interface d'accès

- les PSP gestionnaires de comptes veillent à ce que, sauf en cas d'urgence, toute modification des spécifications techniques de leur interface soit mise à la disposition des autres PSP, **dans les plus brefs délais et au moins trois mois avant la mise en œuvre de la modification**.

### Situations d'urgence

- Les PSP décrivent par écrit les situations d'urgence dans lesquelles les modifications ont été mises en œuvre et mettent cette documentation à la disposition des autorités compétentes sur demande.

# II. Titrisation: évolutions récentes

# RTS spécifiant les exigences pour les initiateurs, les sponsors (institutions financières) et les prêteurs initiaux relativement à la rétention du risque

- **La titrisation est définie dans le Règlement 2017/2402 comme:**
  - Une opération par laquelle, ou un dispositif par lequel, le risque de crédit associé à une exposition ou à un panier d'expositions est subdivisé en tranches

- **Le Règlement 2017/2402 implémente les exigences en matière d'exposition à la titrisation**
  - L'EBA est mandatée, en collaboration avec l'ESMA et l'EIOPA, pour mettre en place des Standards Techniques Règlementaires (RTS) dans ce domaine.
  - La règlementation prévoit que l'EBA soumette ces standards à la Commission au 18 juillet 2018

- **Le but des RTS (EBA/2018/01) est de spécifier dans le détail les exigences de rétention du risque et en particulier (1):**
  - La mesure du niveau de rétention
  - L'interdiction du hedging ou de la vente des intérêts conservés
  - Les conditions de rétention sur une base consolidée

# RTS sur l'homogénéité de l'exposition sous-jacente dans la titrisation et proposant un cadre général pour la titrisation et créant un cadre spécifique pour une titrisation simple, transparente et standardisée

- **Ces RTS (EBA EBA 2018/02) ont été émis en accord avec le Règlement 2017/2402. Ils spécifient plus avant quelle est l'exposition sous-jacente réputée homogène, qui constitue une des exigences relatives à la simplicité, la standardisation et la transparence d'une transaction basée sur la titrisation**

- **L'application de l'exigence d'homogénéité est un prérequis pour un meilleur traitement règlementaire de la sensibilité au risque de la titrisation**

  - La titrisation est adossée à un panier d'expositions sous-jacentes qui sont homogènes en termes de types d'actifs, compte tenu des caractéristiques spécifiques relatives aux flux de trésorerie du type d'actifs, y compris leurs caractéristiques contractuelles, de risque de crédit et de remboursement anticipé
  - Un panier d'expositions sous-jacentes n'est composé que d'un seul type d'actifs
  - Les expositions sous-jacentes incluent des obligations qui sont contractuellement contraignantes et opposables, assorties d'un plein droit de recours à l'encontre des débiteurs et, le cas échéant, des garants

- **L'objectif essentiel de l'exigence d'homogénéité est de permettre aux investisseurs d'évaluer les risques sous-jacents du pool des expositions sous-jacentes sur la base de méthodologies et de paramètres communs. Un ensemble de quatre conditions est établie afin que les expositions sous-jacentes soient considérées comme homogènes:**

  - Elles sont été souscrites d'après des standards de souscription semblables
  - La gestion du sous-jacent doit être obéir à des procédures de gestion semblables, i.e la surveillance, la collecte et la gestion des créances venant de l'exposition sous-jacente à l'actif du SSPE (« Securitisation Special Purpose Entity »: entité de titrisation)
  - Elles appartiennent à la même catégorie d'actif
  - Et pour le majorité des catégories d'actif, elles doivent être homogènes en référence à un moins un facteur d'homogénéité

- **Les RTS spécifient une liste de catégories d'actif ainsi que les listes de facteurs d'homogénéité disponibles pour la majorité des catégories d'actif. Ces catégories reflètent les types les plus habituels d'exposition sous-jacente titrisées dans les pratiques de marché, et incluent:**

  - Créances hypothécaires
  - Créances commerciales
  - Prêts à la consommation
  - Prêts aux entreprises
  - Prêts auto et location longue durée
  - Créances de cartes de crédit
  - Effets de commerce

# RTS sur l'homogénéité de l'exposition sous-jacente dans la titrisation et proposant un cadre général pour la titrisation et créant un cadre spécifique pour une titrisation simple, transparente et standardisée

- **Les facteurs d'homogénéité comprennent:**
  - Le type de débiteur
  - Le rang de priorité des droits sur une propriété
  - Le type de propriété immobilière
  - La juridiction de la propriété / du débiteur
    - A l'exception des effets de commerce et des crédits à la consommation qui sont considérés comme suffisamment homogènes et dans lesquels l'application de facteurs d'homogénéité amènerait à une concentration excessive et non souhaitable dans le pool

# Le cadre français: les nouveaux véhicules de titrisation

- L'ordonnance n°2017-1432 du 4 octobre 2017 instaurait des mesures sur les organismes de financement, les organismes de titrisation et leurs dépositaires

- **Le décret n°2018-1004 du 19 novembre 2018** portant modernisation du cadre juridique de la gestion d'actifs et du financement par la dette:
  - Ce décret précise les conditions dans lesquelles les fonds professionnels spécialisés et les organismes de financement, notamment les organismes de financement spécialisé créés par l'ordonnance n° 2017-1432 du 4 octobre 2017 portant modernisation du cadre juridique de la gestion d'actifs et du financement par la dette, peuvent octroyer des prêts aux entreprises
  - Il permet d'ouvrir cette possibilité de diversification des sources de financement de l'économie, en permettant à de nouveaux acteurs d'octroyer directement des prêts aux entreprises, dans des conditions permettant d'assurer la stabilité du système financier
  - Il précise, en outre, les actifs éligibles aux organismes de financement, la possibilité accordés aux organismes de financement spécialisé d'émettre des obligations, autorise les demandes de rachats, par les investisseurs, de parts, actions ou obligations des organismes de financement spécialisé, modifie certaines dispositions communes aux fonds qui prêtent et contraint les sociétés de gestion gérant des fonds qui prêtent à la réalisation de simulations de crise pour s'assurer de la liquidité des actifs, notamment des prêts octroyés
- **Le décret n°2018-1008 du 19 novembre 2018 portant modernisation du cadre juridique de la gestion d'actifs et du financement par la dette:**
  - Ce décret a pour objet de moderniser le cadre juridique de la gestion d'actifs et du financement par la dette. Il complète le dispositif de diversification des sources de financement de l'économie, en permettant à de nouveaux acteurs d'octroyer directement des prêts aux entreprises, dans des conditions garantissant la stabilité du système financier
  - Le texte précise les conditions dans lesquelles les organismes de financement, créés par l'ordonnance n° 2017-1432 du 4 octobre 2017 portant modernisation du cadre juridique de la gestion d'actifs et du financement par la dette, peuvent octroyer des prêts aux entreprises
  - Il précise les modalités d'acquisition et de cession de créances par un organisme de financement

# III. Gouvernance : Orientations EBA/GL/2017/12 & ESMA / EBA 21 mars 2018

## ❑Notice de conformité de l'ACPR du 5 juin 2018 aux orientations EBA relatives à la gouvernance interne (EBA/GL/2017/12)

L'ACPR entend se conformer pleinement aux orientations sur la gouvernance interne du 26 septembre 2017. Elle s'attend à ce que celles-ci soient mises en œuvre par les établissements de crédit et les entreprises d'investissement.

L'ACPR attend également que les sociétés de financement, qui n'entrent pas dans la définition des « établissements financiers » visés au paragraphe 1 de l'article 4 du règlement (UE) n°1093/2010 instituant l'EBA mais auxquelles s'appliquent les exigences de la directive CRDIV relatives à la gouvernance, mettent en œuvre les orientations.

# Les principales fonctions de surveillance de l'organe de direction [EBA/GL/2017/12]

| |
|---|
| Superviser et suivre la prise de décisions et les actions de la direction et assurer une surveillance efficace de l'organe de direction dans sa fonction exécutive, y compris en suivant et en étudiant ses performances individuelles et collectives et la mise en œuvre de la stratégie et des objectifs de l'établissement. |
| Remettre en question de manière constructive et examiner d'un œil critique les propositions et les informations fournies par les membres de l'organe de direction dans sa fonction exécutive ainsi que ses décisions. |
| En tenant compte du principe de proportionnalité, remplir de manière appropriée les attributions et le rôle du comité des risques, du comité de rémunération et du comité de nomination, lorsque ces comités n'ont pas été instaurés. |
| Garantir et évaluer périodiquement l'efficacité du cadre de gouvernance interne de l'établissement et prendre des mesures appropriées afin de remédier aux éventuelles faiblesses détectées. |
| Superviser et suivre la mise en œuvre de manière cohérente des objectifs stratégiques, de la structure organisationnelle et de la stratégie en matière de risque de l'établissement, y compris son appétit pour le risque et son cadre de gestion des risques, ainsi que d'autres politiques (par exemple, la politique de rémunération) et le cadre de publication d'informations. |
| Contrôler que la culture du risque de l'établissement est mise en œuvre de manière cohérente. |
| Superviser la mise en œuvre et le maintien d'un code de conduite ou de politiques similaires et efficaces visant à détecter, gérer et atténuer les conflits d'intérêts avérés et potentiels. |
| Superviser l'intégrité des informations financières et des rapports financiers ainsi que le cadre de contrôle interne, y compris un cadre efficace et sain de gestion des risques. |
| Garantir que les responsables des fonctions de contrôle interne sont en mesure d'agir de manière autonome et, indépendamment de la responsabilité de rendre des comptes à d'autres organes internes, lignes d'activité ou unités, peuvent exprimer leurs préoccupations et avertir l'organe de direction dans sa fonction de surveillance directement, le cas échéant, lorsque des risques d'évolutions défavorables affectent ou sont susceptibles d'affecter l'établissement. |
| Suivre la mise en œuvre du plan d'audit interne, après la participation préalable des comités des risques et d'audit, lorsque ces comités sont instaurés. |

## Organisation des comités :

- Tous les comités devraient être présidés par un membre de l'organe de direction n'exerçant pas de fonctions exécutives, capable d'exercer un jugement objectif.
- Les membres indépendants de l'organe de direction dans sa fonction de surveillance devraient participer activement aux comités.
- Lorsque des comités devraient être composés d'au moins trois membres.
- Les établissement devraient s'assurer, que les comités ne sont pas composés du même groupe de membres formant un autre comité.
- Les établissements devraient envisager la rotation périodique des présidents et membres des comités, en tenant compte de l'expérience, des connaissances et des compétences spécifiques requises à titre individuel ou collectif pour ces comités.
- Chaque comité doit recevoir un mandat écrit, précisant la portée de ses responsabilités, de la part de l'organe de surveillance.
- Chaque comité doit établir des procédures de travail appropriées ;

## Rôle du Président de l'organe de surveillance

L'EBA (Orientations 2017/11) précise les missions du président de l'organe de surveillance :

⇒ Contribuer à un flux d'information efficace au sein de l'organe de surveillance, entre ses différents comités et avec les dirigeants effectifs.

⇒ Encourager et favoriser les discussions ouvertes et critiques, en s'assurant que les opinions divergentes peuvent être exprimées et débattues dans le cadre de la prise de décision.

⇒ Etablir l'ordre du jour des réunions et assurer que les questions stratégiques sont discutées prioritairement.

⇒ Pour que les décisions soient prises de manière éclairée, il s'assure que les documents et les informations ont été reçus dans un délais suffisant avant les réunions.

⇒ Il participe à une répartition claire des attributions entre les différents membre de l'organe de surveillance pour permettre à ses membres de contribuer de manière constructive aux discussions et de voter de manière judicieuse et éclairée.

## Rôle du comité des risques (Orientations EBA 2017/11)

Supervise de la mise en œuvre des stratégies de l'établissement :

- Gestion des fonds propres
- Gestion du risque de liquidité
- Gestion du risque de marché
- Gestion du risque de crédit
- Gestion du risque opérationnel (y compris les risques juridiques et informatiques)
- Gestion du risque de réputation
- Examen de scénarios de tension (Stress tests).
- Adéquation des produits et services financiers proposés avec la stratégie en matière de risques .
- Evaluation des recommandations des auditeurs internes ou externes et suivi de la mise en œuvre des mesures adoptées.
- Examen des pratiques de rémunérations, pour qu'elles prennent en compte le risque (capital et liquidité) de l'établissement.

Reçoit :

- Informations et données pertinentes y compris de la part des fonctions opérationnelles ou de contrôle.
- Rapports réguliers et informations de la part des responsables du contrôle interne sur le profil de risque, la culture du risque et les limites de risque de l'établissement ainsi que toute violation significative et les mesures correctives proposées.

Fournit à l'organe de supervision :

- Conseil et assistance en matière de risques et d'appétit au risque en prenant en compte tout les types de risques.
- Une assistance pour la supervision de la mise en œuvre de la politique de risque.
- Recommandations sur les ajustements nécessaires à apporter à la politique en matière de risques.
- Conseil concernant le recrutement de consultants externes en vu d'obtenir des avis ou une assistance.

❑Notice de conformité de l'ACPR du 5 juin 2018 aux orientations EBA sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés EBA/GL/2017/12.

L'ACPR entend se conformer **partiellement** aux orientations sur l'évaluation de l'aptitude, **à l'exception des dispositions prévoyant l'évaluation par l'autorité de supervision de l'aptitude des titulaires de postes clés à chaque nomination ou renouvellement**.

La déclaration de non-conformité s'applique aux **paragraphes suivants :**

- **P.162 :** Les établissements CRD ayant une importance significative, devraient informer les autorités compétentes des résultats de l'évaluation concernant les responsables de fonctions de contrôle interne et le directeur financier, lorsqu'ils ne font pas partie de l'organe de direction.
- **P.176 :** Les établissements CRD ayant une importance significative, pour lesquels une évaluation des responsables de fonctions de contrôle interne et du directeur financier, lorsqu'ils ne font pas partie de l'organe de direction, est requise (Cf. 171 et 172), devraient notifier aux autorités compétentes la nomination de ces fonctions sans tarder et au plus tard dans un délai de deux semaines à compter de leur nomination**.**
- **P.171 et 172 :** Les responsables de fonctions de contrôle interne et le directeur financier nouvellement nommés, lorsqu'ils ne font pas partie de l'organe de direction, sont évalués par les autorités compétentes.

❑Notice de conformité de l'ACPR du 5 juin 2018 aux orientations EBA sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés EBA/GL/2017/12.

Par ailleurs, l'ACPR entend appliquer les orientations relatives à la présence et la définition de membres indépendants avec réserves d'interprétation :

- L'indépendance formelle des membres de l'organe de direction et des membres du comité des risques et du comité des nominations ne constitue pas un critère d'aptitude prévu par la législation et la règlementation française en vigueur, qui serait opposable dans le cadre de l'examen d'une candidature individuelle. En droit français, la mise en œuvre des orientations ne saurait donc conduire au refus sur ce seul motif d'une candidature individuelle au titre du « fit and proper».
- Par ailleurs, hormis le cas spécifique des comités d'audit des entités d'intérêt public, pour lesquels l'article L. 823-19 du code de commerce prévoit, en principe, la présence d'un administrateur indépendant, au titre de la transposition de la Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés, **l'ACPR considère la présence de membres indépendants, au sein des organes de surveillance et autres comités spécialisés comme relevant de bonnes pratiques à encourager et non d'une exigence légale ou règlementaire**.

❑Notice de conformité de l'ACPR du 5 juin 2018 aux orientations EBA sur l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés EBA/GL/2017/12.

En application du paragraphe 89)b) des orientations sur l'évaluation de l'aptitude, **l'ACPR entend également ne pas exiger la présence de membres indépendants dans les établissements CRD entièrement détenus par un établissement CRD et dans les établissements CRD n'ayant pas d'importance significative qui sont des entreprises d'investissement.**

**L'ACPR s'attend à ce que les orientations auxquelles elle déclare se conformer soient mises en œuvre par les établissements de crédit, les entreprises d'investissement, les compagnies financières holding et les compagnies financières holding mixtes.**

**L'ACPR attend également que les sociétés de financement, qui n'entrent pas dans la définition des « établissements financiers » visés au paragraphe 1 de l'article 4 du règlement (UE) n°1093/2010 instituant l'ABE mais auxquelles s'appliquent les exigences de la directive CRDIV relatives à la gouvernance, mettent en œuvre les orientations.**

**Position AMF (Doc-2018-08) concernant les orientation conjointes de l'Autorité Bancaire Européenne (« ABE ») et de l'Autorité Européennes des Marchés Financiers (« AEMF ») relatives à l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires des postes clés (EBA/GL/2017/12) . Ces orientations s'appliquent depuis le 30 juin 2018.**

❖ L' Autorité des marchés financiers « AMF », a déclaré le 29 mai 2018 se conformer, (**tout comme l'ACPR, partiellement)** aux orientations conjointes de l'Autorité Bancaire Européenne « ABE » et l'Autorité Européenne des Marchés Financiers « AEMF » relatives à l'évaluation de l'aptitude des membres de l'organe de direction et des titulaires de postes clés (EBA/GL/2017/12) à l'exception des paragraphes 162, 171, 172 de ces orientations pour les raisons précisées ci-dessous :

Ces orientations définissent les exigences concernant l'aptitude des membres de l'organe de direction des établissements de crédit (« EC ») et des entreprises d'investissement (« EI »). Elles explicitent notamment les notions de :

- Temps suffisant consacré à l'exercice de leur fonction par les membres de l'organe de direction ;
- Honnêteté, intégrité, indépendance d'esprit dont doivent faire preuve les membres de l'organe de direction ;
- Connaissances, compétences, expérience dont dispose collectivement l'organe de direction ;
- Ressources humaines et financières adéquates à consacrer à l'initiation et à la formation des membres de l'organe de direction ;
- Diversité, à prendre en compte pour la sélection des membres de l'organe de direction.

« Position AMF Doc-2018-08 _ Document créé le 26 mai 2018 »

**La notion de « Réputation, honnêteté et intégrité dont doivent faire preuve les membres de l'organe de direction » :**

- Sans préjudice des éventuels droits fondamentaux, tous les antécédents judiciaires ou administratifs doivent être pris en compte pour évaluer l'honorabilité, l'honnêteté et 'intégrité, en considérant le type de condamnation ou de mise en accusation, le rôle de la personne concernée, la peine imposée, le stade de la procédure judiciaire atteint et les éventuelles mesures de réinsertion mises en place. Tous les antécédents judiciaires ou administratifs pertinents doivent être pris en compte en considérant les délais de prescription applicables en vertu du droit national.
- Sans préjudice de la présomption d'innocence applicable aux procédures pénales et des autres droits fondamentaux, les facteurs suivants doivent, à tout le moins, être considérés lors de l'évaluation de la réputation, de l'honnêteté et de l'intégrité :

  a. toute condamnation ou poursuite en cours pour infraction pénale;

  b. toute autre mesure pertinente actuelle ou passée adoptée par un organe réglementaire ou professionnel pour non-respect des dispositions pertinentes régissant les activités bancaire, financière, de valeur immobilières ou d'assurance.

« ORIENTATIONS SUR L'EVALUATION DE L' APTITUDE DES MEMBRES DE L'ORGANE DE DIRECTION ET DES TITULAIRES DE POSTES CLES _ Document EBA_21/03/2018 »

**La notion de « Réputation, honnêteté et intégrité dont doivent faire preuve les membres de l'organe de direction » :**

- Les enquêtes en cours doivent être prises en compte lorsqu'elles résultent de procédures judiciaires ou administratives ou d'autres enquêtes réglementaires similaires, sans préjudice des droits fondamentaux individuels.
- Les situations ci-dessous se rapportant aux performances commerciales passées et actuelles et à la solidité financière d'un membre de l'organe de direction doivent être considérées en rapport avec leur incidence potentielle sur la réputation, l'intégrité et l'honnêteté du membre :

a. le fait d'être un débiteur défaillant (par exemple, avoir un dossier négatif auprès d'une société d'information financière fiable, le cas échéant);

b. les performances financières et commerciales des entités détenues ou dirigées par le membre ou dans lesquelles ce dernier avait ou à une participation ou une influence importante, en examinant en particulier toute procédure de faillite ou liquidation et si et dans quelle mesure le membre a contribué à la situation ayant conduit à la procédure;

c. toute déclaration de faillite personnelle; et

d. sans préjudice de la présomption d'innocence, actions civiles en justice, procédures administratives ou pénales, investissements ou expositions et emprunts importants, dans la mesure où ils peuvent avoir une incidence significative sur la solidité financière du membre ou des entités détenues ou dirigées par le membre ou dans lesquelles le membre détient une participation significative.

« ORIENTATIONS SUR L'EVALUATION DE L' APTITUDE DES MEMBRES DE L'ORGANE DE DIRECTION ET DES TITULAIRES DE POSTES CLES _ Document EBA_21/03/2018 »

**La notion de « Réputation, honnêteté et intégrité dont doivent faire preuve les membres de l'organe de direction » :**

- Un membre de l'organe de direction doit préserver des normes élevées d'intégrité et d'honnêteté. À tout le moins, les établissements doivent également considérer les facteurs suivants lorsqu'ils évaluent la réputation, l'honnêteté et l'intégrité :

  a. tout signe que la personne ne s'est pas montrée transparente, ouverte et coopérative dans ses interactions avec les autorités compétentes;

  b. tout refus, révocation, annulation ou renvoi de tout enregistrement, agrément, adhésion ou licence permettant d'exercer un métier, une activité ou une profession;

  c. les raisons de tout licenciement ou de toute destitution d'un poste de confiance, d'une relation fiduciaire ou d'une autre situation similaire, ainsi que de toute demande de démission d'un tel poste;

  d. l'interdiction imposée par toute autorité compétente pertinente de faire partie des membres de l'organe de direction, y compris des personnes qui dirigent effectivement les activités d'une entité; et

  e. toute autre preuve suggérant que la personne agit de manière non conforme à des normes de conduite élevées.

« ORIENTATIONS SUR L'EVALUATION DE L' APTITUDE DES MEMBRES DE L'ORGANE DE DIRECTION ET DES TITULAIRES DE POSTES CLES _ Document EBA_21/03/2018 »

## La notion de « Indépendance d'esprit des membres de l'organe de direction » :

❖ Lorsqu'ils évaluent l'indépendance d'esprit, les établissements devraient évaluer si les membres de l'organe de direction:

a. possèdent les aptitudes comportementales nécessaires, y compris:

i. le courage, la conviction et la force d'évaluer efficacement et de remettre en cause les décisions proposées par d'autres membres de l'organe de direction;

ii. la capacité de poser des questions aux membres de l'organe de direction dans sa fonction exécutive; et

iii. la capacité de résister au conformisme de groupe;

b. sont influencés par des conflits d'intérêts dans une mesure qui porterait atteinte à leur capacité d'exercer leurs fonctions de manière indépendante et objective.

« ORIENTATIONS SUR L'EVALUATION DE L' APTITUDE DES MEMBRES DE L'ORGANE DE DIRECTION ET DES TITULAIRES DE POSTES CLES _ Document EBA_21/03/2018 »