Bird & Bird

Atelier :

Le défi de la fraude dans le secteur bancaire, enjeux et solutions

Aspects juridiques et réglementaires de la protection des données et paiements

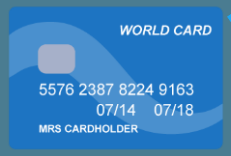
Merav Griguer
Avocate associée

Les points clés de la protection des données financières

1. Les données bancaires et financières au regard de la DSP2

2. Les données bancaires et financières au regard du RGPD

Bird & Bird



1. Les données bancaires et financières au regard de la DSP2

Bird & Bird

Les acteurs dans le secteur bancaire et financier

- **Anciens acteurs :**
  - **Prestataires de services de paiement gestionnaires de comptes (les « PSPGC ») :**
    - Il s'agit principalement des établissements de crédit ou banques

- **Nouveaux acteurs :**
  - **Prestataires de service de paiement tiers aux comptes (les « PSPTC ») :**
    - **les Prestataires de services d'initiation de paiement (les « PSIP »)** : par exemple, Slimpay ou Soforbanking
    - **les Prestataires de services d'information sur les comptes (les « PSIC »)** : par exemple, Linxo ou Budget Insight

Bird & Bird

Pourquoi la DSP2 a t-elle était adoptée ?

- **Problème :**
  - Les **PSPTC** se sont développés **en dehors de tout cadre réglementaire**
  - Recours à une pratique dénommée le ***Web Scraping*** *:* consiste à **se connecter sur le site de la banque à distance du client en se faisant passer pour ce dernier** (**communication de ses identifiants + codes confidentiels**) **et à récupérer les données disponibles sur ses comptes bancaires**

Risque de fraude !!

Rappel chronologique de l'adoption de la DSP2

Etape 1

Adoption de la DSP2 le 25 novembre 2015

Etape 2

Transposition de la DSP2 en droit français

(ordonnance du 9 août 2017 + loi de ratification du 3 août 2018)

Etape 3

Article 98 DSP2

Adoption de mesures de sécurité ou "NTR" (Normes techniques de réglementation) avec Règlement délégué du 27 novembre 2017

Etape 4

Authentification forte du client

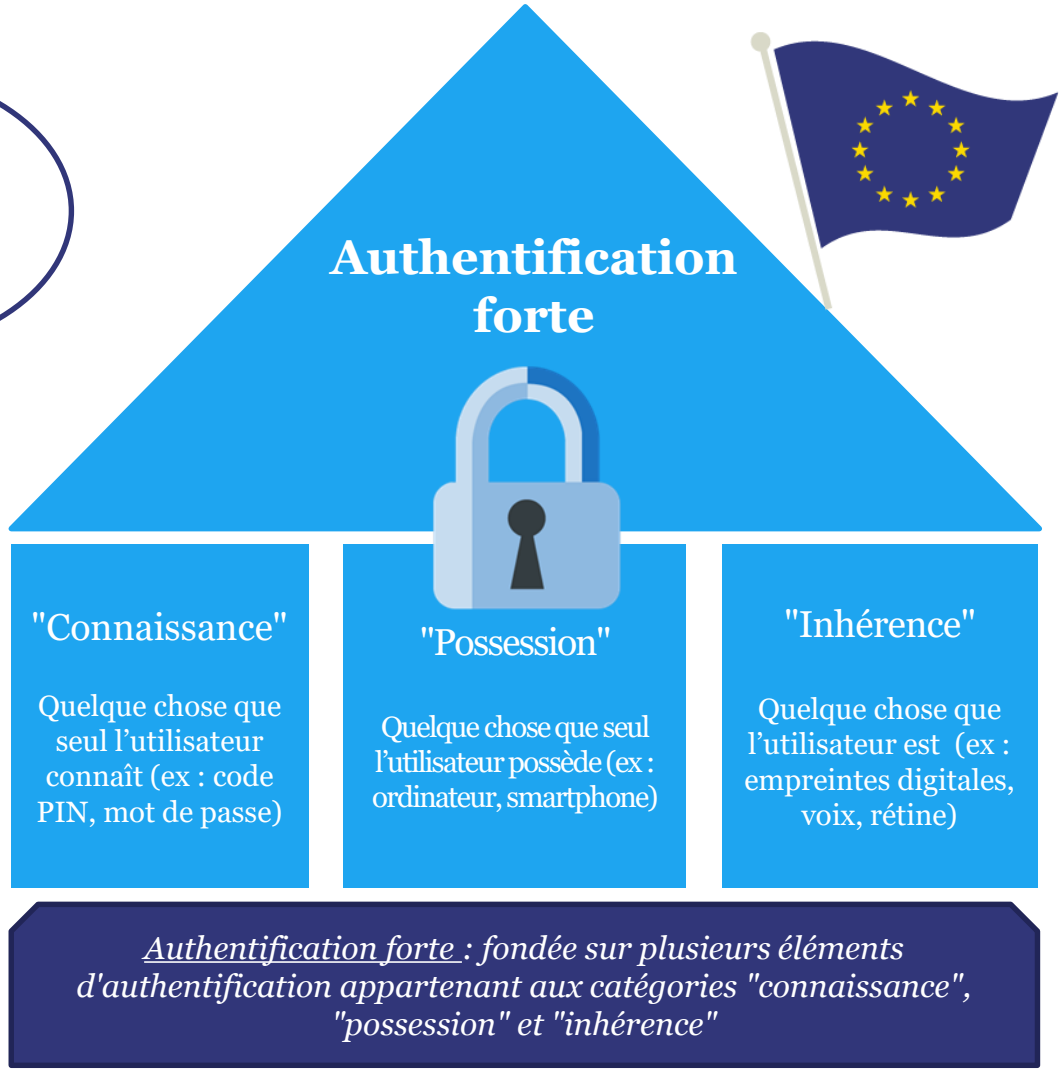
Date d'entrée en application initiale : 14 septembre 2019

Report de la date d'entrée en application : 31 décembre 2020

Bird & Bird

Qu'est ce que l'authentification forte du client ?

Cons. 30 DSP2
&
art. 4§1
Règlement
délégué



Bird & Bird

Quelles règles à retenir sur l'authentification forte ?

Utilisation d'au moins 2 éléments d'authentification

Ex : l'utilisation exclusive de la réponse à une question secrète serait insuffisante

Répondre aux catégories "connaissance", "possession" et "inhérence"

Ex : l'utilisation d'un code confidentiel envoyé par SMS de type 3D Secure V1 serait insuffisante (car principe d' "inhérence" ferait défaut)

Bird & Bird

Illustrations des mesures de sécurité garantissant l'authentification forte

- « aucune information sur l'un des éléments [d'authentification] (…) ne peut être déduite de la divulgation du code d'authentification »
- « il n'est pas possible de générer un nouveau code d'authentification en se basant sur un autre code d'authentification généré au préalable » et « le code d'authentification ne peut pas être falsifié »
- dans le cadre d'un accès à distance, si l'authentification « n'a pas généré de code d'authentification », il ne doit pas être possible de connaitre l'élément d'authentification qui était incorrect

Art. 4§2 & §3 Règlement délégué

- *Ex : un tiers prend connaissance du code confidentiel d'un client et pourrait ensuite en déduire ses coordonnées bancaires*
- *Ex : un PSP créé un code confidentiel pour son client en reprenant un de ses codes antérieurs*
- *Ex : achat effectué via technologie 3D Secure V1, le prétendu acheteur ne doit pas savoir que c'est une erreur liée à l'inscription du cryptogramme visuel à 3 chiffres qui l'a empêché de recevoir le SMS contenant le code confidentiel*

Illustrations des mesures de sécurité garantissant l'authentification forte

Art. 4§3 & 5 Règlement délégué

- « le nombre de tentatives d'authentification infructueuses consécutives (…) ne dépasse pas 5 au cours d'une période donnée »
- « les sessions de communication sont protégées contre l'interception des données d'authentification communiquées durant l'authentification et contre la manipulation par des tiers non autorisés »
- « le délai maximal d'inactivité du payeur, une fois que celui-ci s'est authentifié pour accéder à son compte de paiement en ligne, ne dépasse pas 5 minutes ».
- Le Règlement délégué exige l'établissement d'un « lien dynamique » entre le client et l'opération de paiement projetée, à ce titre, il est notamment prévu que :
  - le payeur soit informé du montant de l'opération projetée et de l'identité du bénéficiaire,
  - le code d'authentification soit spécifique au montant de l'opération projetée et au bénéficiaire, et
  - le code d'authentification corresponde au montant spécifique initial de l'opération projetée et à l'identité du bénéficiaire.

Bird & Bird

Dans quels cas peut-on déroger à l'authentification forte du client ?

Les dispenses relatives à certaines informations sur le compte de paiement

Si l'accès du PSP est limité à 1 ou 2 des éléments suivants :

- le solde d'un ou de plusieurs comptes de paiement désignés,
- les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.

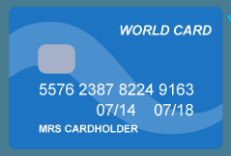
Les dispenses relatives à certaines opérations de paiement courantes

- les virements effectués entre des comptes détenus par la même personne,
- les paiements effectués par carte bancaire sans contact,
- les opérations de faible valeur effectuées à distance, et
- les opérations présentant un faible niveau de risque.

Les dispenses relatives à certaines listes spécifiques de paiements

- les PSP sont tenus de recourir à une authentification forte pour créer ou modifier des **listes de bénéficiaires de confiance** ou de créer, modifier ou initier pour la 1ère fois des **listes d'opérations récurrentes**,
- Mais ils en sont dispensés pour toute initiation d'opérations de paiement relatives à ces 2 listes.

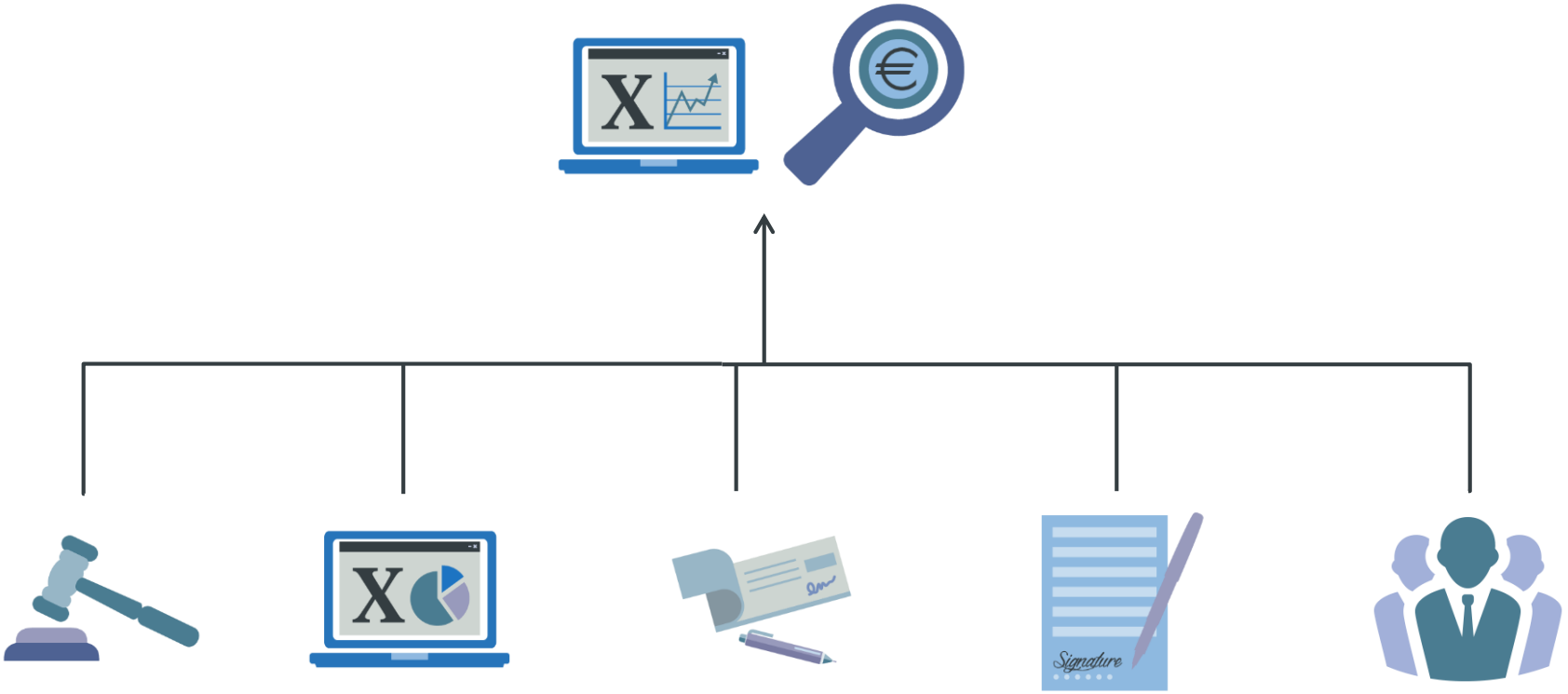
Art. 13 & 14 Règlement délégué



2. Les données bancaires et financières au regard du RGPD

Bird & Bird

Données bancaires et financières



Lutte contre la fraude

Scoring

Lutte contre le blanchiment

Accès au Répertoire National d'Identification des Personnes Physiques (RNIPP)

Gestion des listes d'initiés

Bird & Bird

Normes simplifiées & Autorisations Uniques pour le secteur bancaire

AVANT RGPD

- **Normes simplifiées**
  - **NS12** : Tenue des comptes bancaires des clients
  - **NS13** : Gestion des crédits aux personnes physiques
  - **NS41** : Gestion des instruments financiers
- **Autorisations Uniques**
  - **AU03**: Lutte contre le blanchiment par les organismes financiers
  - **AU05**: Système d'aide à l'octroi de crédit
  - **AU45**: Consultation du RNIPP
  - **AU54** : Lutte contre la fraude externe dans le secteur bancaire et financier
- **Dispenses de Déclarations**
  - **DI09**: Gestion des listes d'initiés

RGPD

- Suppression de l'ensemble de ces normes, autorisations et dispenses
- Registre des activités de traitement
- PIA

Exemples de catégories de données collectées : numéro de carte bancaire, cryptogramme, domiciliation bancaire, encours de l'épargne, montant du solde des comptes, crédits détenus, incidents de paiements, fréquence d'utilisation des moyens de paiements, etc.

Les données de cartes bancaires

- **Application du principe de minimisation :**
  - **Minimisation des données** :
    - Numéro de la carte, date d'expiration et cryptogramme visuel
    - Identité du titulaire de la carte : uniquement si justifiée (ex : lutte contre la fraude)
    - Copie du recto et/ou verso de la carte de paiement : non autorisée
  - **Minimisation de la durée de conservation** :
    - Pas de conservation au-delà de la transaction (sauf abonnement)
    - Peuvent être conservées en archivage (sauf le cryptogramme visuel) à des fins de gestion des réclamations 13 mois (ou 15 mois en cas de débit différé)

- **Mesures de sécurité :** masquage de tout ou partie du numéro de la carte, remplacement du numéro de carte par un numéro non signifiant, traçabilité des accès ou utilisation illégitime des données.

Bird & Bird

Merci & Bird & Bird

Merav Griguer
Avocate associée

twobirds.com