Conformité Réglementaire

1. RGPD (Protection des Données Personnelles)

La gestion des données des étudiants et des transactions financières repose sur un principe strict de **minimisation**, garantissant que seules les informations essentielles au fonctionnement du wallet et du moteur de fraude sont collectées. Pour répondre aux obligations de traçabilité et permettre des audits historiques, le système assure la **rétention des logs de décision** (incluant les scores de fraude et les motifs de validation ou de rejet) pendant une durée de **7 ans**. En complément, des procédures d'**anonymisation** sont systématiquement mises en œuvre lorsque cela est possible afin de protéger l'identité des utilisateurs tout en préservant la valeur analytique des données pour l'amélioration des modèles.

2. PSD2 (SCA Dynamique)

Afin de respecter la Directive sur les Services de Paiement 2, la sécurité des échanges est renforcée par l'intégration native d'une **authentification forte du client (SCA)**. Ce mécanisme d'authentification est **dynamique**, ce qui signifie qu'il est déclenché ou intensifié en fonction du **score de risque calculé en temps réel** par le moteur de fraude hybride, lequel combine l'intelligence artificielle et des règles métier spécifiques au milieu étudiant.

3. PCI-DSS (Sécurité des Données Bancaires)

La protection des informations de paiement au sein des campus est assurée par l'application rigoureuse des standards de l'industrie, notamment via la **tokenisation** qui remplace les données sensibles des cartes bancaires par des jetons sécurisés au lieu de les stocker en clair. Toutes les données persistantes, qu'elles soient dans le ledger transactionnel ou les bases de données SQL, font l'objet d'un **chiffrement At-Rest** systématique. Par ailleurs, par souci de conformité et de sécurité, le système interdit formellement tout stockage du code de vérification (**CVV**).

4. ACPR (Contrôle et Audit)

Pour satisfaire aux exigences de l'Autorité de Contrôle Prudentiel et de Résolution, le système garantit une **traçabilité totale et infalsifiable** des opérations. Les journaux de transactions et de décisions sont rendus immuables grâce à une **signature numérique** utilisant l'algorithme **HMAC-SHA256**. Cette architecture permet de générer des **rapports d'audit complets** à la demande, facilitant ainsi grandement les contrôles réglementaires officiels ou les audits internes de l'établissement.

5. AML/KYC (Lutte contre le Blanchiment)

Bien que Carte Blanche soit un portefeuille numérique dédié à l'usage étudiant et associatif, il intègre des mesures de vigilance bancaire proportionnées. Le système prévoit un **screening des listes noires** pour filtrer les utilisateurs par rapport aux listes de sanctions internationales, ainsi qu'une vérification des **Personnes Politiquement Exposées (PEP)** lorsque le contexte de l'utilisateur le justifie. Ces dispositions garantissent que la solution n'est pas seulement un outil de fidélisation, mais une plateforme Fintech robuste et sécurisée.

6. Aspect Économique (TVA)

Conclusion

En conclusion, le projet "Carte Blanche" se distingue par sa capacité à transformer un outil de vie étudiante en une **plateforme Fintech hautement sécurisée**. En intégrant dès sa conception les exigences du RGPD, de la PSD2 et des standards PCI-DSS, il offre une réponse concrète aux besoins de modernisation des Bureaux des Élèves (BDE) et des directions d’établissements. L’innovation majeure réside dans son **moteur de fraude hybride**, capable d’assurer l’intégrité des transactions tout en restant scalable pour gérer jusqu'à 10 000 transactions par jour.

Ce positionnement unique, à l'intersection de l'EdTech et de la Fintech, permet non seulement de sécuriser les flux financiers des campus mais aussi de valoriser l'engagement étudiant à travers un système de fidélisation innovant. Grâce à cette rigueur réglementaire et technique, Carte Blanche s'affirme comme une solution viable, pérenne et prête à être déployée à l'échelle nationale, voire européenne.