Amélioration des notifications : Assurer que les notifications de transaction soient envoyées indépendamment de l'accès des employés.

Implémentation de l'authentification biométrique : Utiliser des empreintes digitales ou la reconnaissance faciale pour valider les transactions.

Système de double validation : Chaque transaction nécessite la confirmation du client avec un code unique.

Feedback en Temps Réel : Offrir des notifications instantanées pour chaque étape de la transaction.

Personnalisation des Alertes : Permettre aux utilisateurs de choisir les types d'alertes qu'ils souhaitent recevoir.

Système de Détection des Fraudes : Mise en place d'algorithmes d'IA pour détecter les comportements suspects en temps réel.

Audits réguliers : Mettre en place des audits internes fréquents pour détecter toute anomalie.

Formation des employés : Former les employés sur l'importance de la sécurité des données et des transactions.

Campagnes de sensibilisation : Informer les utilisateurs sur les méthodes de sécurité disponibles et les arnaques potentielles.

Éducation sur la Sécurité : Offrir des ressources éducatives en ligne sur la sécurité des transactions et la protection des données.

Campagnes de Sensibilisation : Lancer des campagnes pour informer les utilisateurs sur la sécurité de leurs données et les comportements à adopter.

Support Client Amélioré : Mettre en place un support client réactif et accessible pour répondre aux préoccupations de sécurité des utilisateurs.

Améliorer l'Interface Utilisateur (UI) : Simplifier le processus de transaction pour le rendre plus intuitif.

Feedback en Temps Réel : Offrir des notifications instantanées pour chaque étape de la transaction.

Personnalisation des Alertes : Permettre aux utilisateurs de choisir les types d'alertes qu'ils souhaitent recevoir.

Alliances avec des Fournisseurs de Sécurité : Collaborer avec des entreprises spécialisées en cybersécurité pour améliorer les systèmes de protection.

Partenariats avec des Banques : Travailler avec des institutions financières pour partager des données sur les fraudes et les meilleures pratiques de sécurité.

Programmes de Formation Communautaire : Établir des partenariats avec des organisations locales pour sensibiliser et éduquer les utilisateurs sur la sécurité des transactions.

Application de Sécurité : Développer une application dédiée qui permet aux utilisateurs de gérer leurs alertes de sécurité et d'activer des fonctionnalités de sécurité.

Dispositifs de Sécurité Physiques : Proposer des dispositifs physiques (comme des clés de sécurité) pour les transactions sensibles.

Options de Récupération : Création de mécanismes de récupération des comptes en cas de fraude, avec une authentification renforcée.