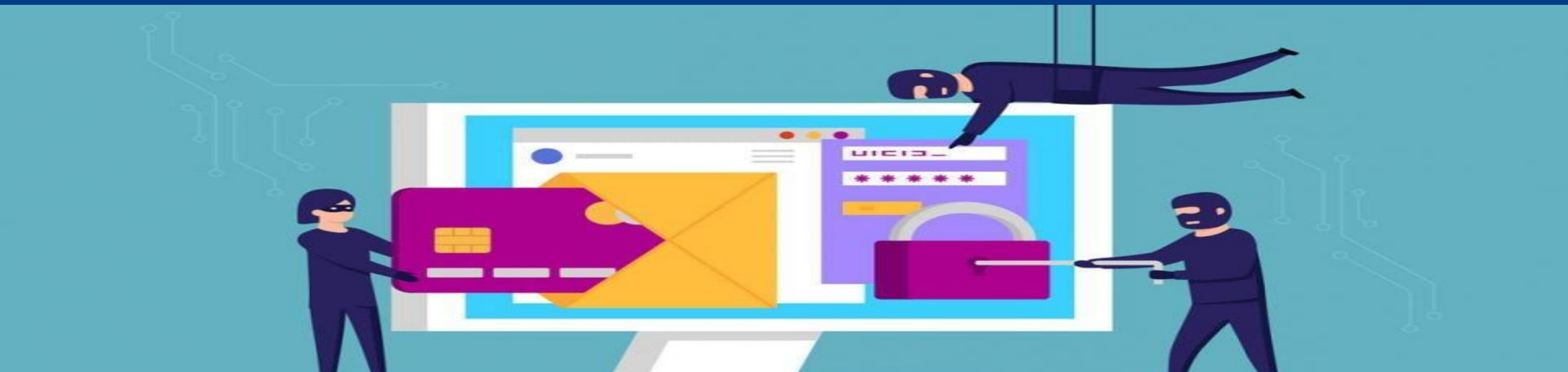
Atelier 3

LUTTE CONTRE LA FRAUDE MODERNE: DÉTECTER LES FRAUDES MODERNES ET SÉCURISER LA BANQUE

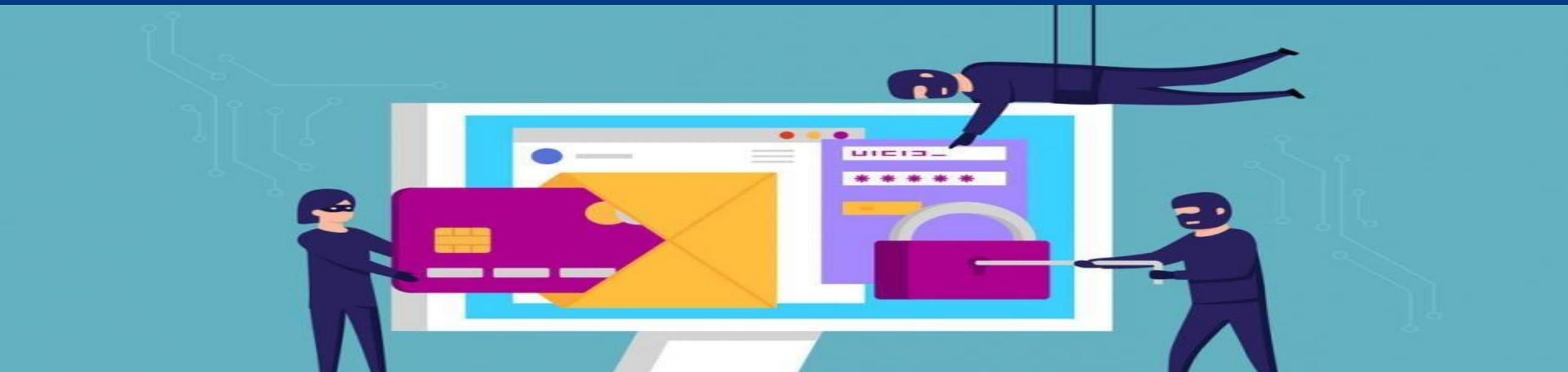
Expert, animateur :

Dr Magloire SOSSOUVI, *Expert en gouvernance bancaire et lutte contre la fraude moderne en banque*

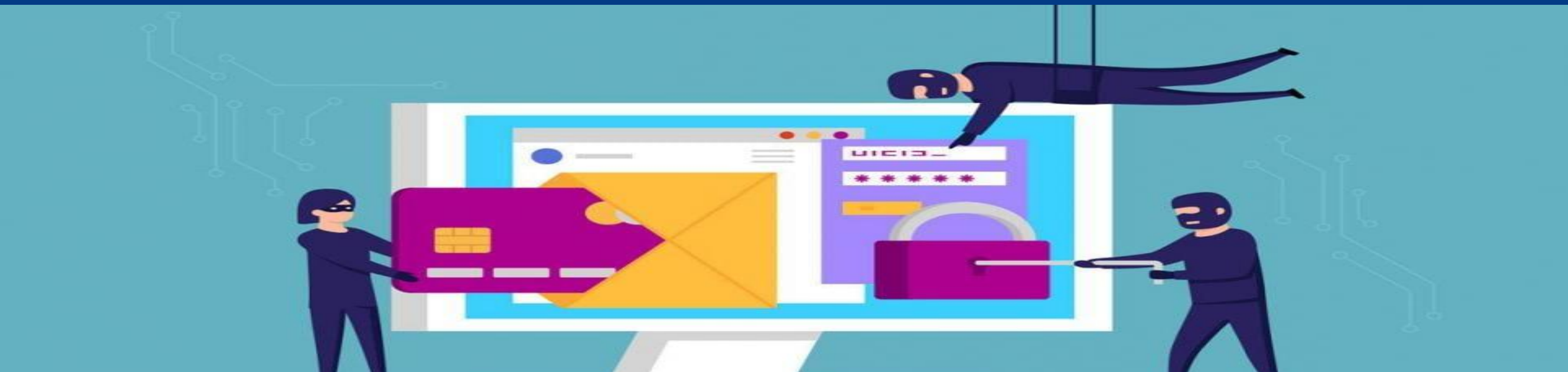
De manière générale, la fraude se définit par l'usage d'un faux nom, d'une fausse qualité, d'abus d'une qualité vraie ou des manœuvres frauduleuses pour déterminer la remise d'une valeur (article 313-1 du Code Pénal).



La fraude par le numérique se définit par l'utilisation d'outils informatiques et de réseaux pour commettre des infractions, notamment par l'accès frauduleux à un système de traitement automatisé de données, la modification des données, le vol d'informations ou l'escroquerie en ligne.



Le perimetre des actes utilisés est de plus en plus large et sophistiqué.
Par analyse d'origine et par impact, la typologie des fraudes fait ressortir des fraudes qualifiés internes et d'autres externes.



Qualificatif	Fraude interne	Fraude externe
AUTEUR	Provient de l’intérieur de la banque.	Provient d’une personne ou d’un groupe extérieur à la banque (client, fournisseur, hacker.).
EXEMPLES	Détournement, corruption, manipulation des comptes, des écritures, falsification des documents, usage abusif des ressources informatiques.	Fraude à la carte bancaire, escroquerie au faux prestataire, cyber-attaque, phishing, vol d’identité, usurpation d’actes.
RISQUES ASSOCIES	Perte de confiance de l’employeur.	Risque de réputation, procès avec le client, plainte du client contre la banque à la Commission Bancaire.
OBJECTIF	Obtenir un gain personnel ou avantager des tiers.	Tirer un profit indu de la banque.

<u>La fraude par piratage de compte</u>	**La fraude au virement bancaire**
	La fraude aux paiements
<u>La compromission de la messagerie d’entreprise</u>	
La fraude à la relation amoureuse	La fraude aux paiements en temps réel (RTP)
La fraude aux sentiments	La fraude aux dépôts au DAB
<u>La fraude envers les personnes âgées</u>	La fraude au retrait au DAB
L’escroquerie au travail à domicile	La fraude au chèque

La fraude au PDG	**La fraude aux fonds d'investissement immobilier**
La fraude par triangulation	**La fraude au titre de propriété**
La fraude interne en entreprise	**La fraude hypothécaire**
La fraude aux produits et services	La fraude au chèque déposé via une application mobile
L'escroquerie à l'accusation de fraude fiscale	La fraude au numéro de chèque dupliqué
L'escroquerie à l'imposteur de la sécurité sociale	La fraude au numéro de chèque erroné
L'escroquerie au voyage	**La fraude au retour**
L'escroquerie aux faux articles	La fraude au chèque volé/copié

La fraude à la fausse facture	**La fraude au chargeback frauduleux (fraude à la retrofacturation)**
	L’arnaque à l’avance de frais
La fraude aux paiements push autorisés (APP)	L’escroquerie médicale
La fausse déclaration	La fraude à l’acquéreur (commerçant)
La fraude à l’identité synthétique	La fraude au faux commerçant
La fraude à la carte de crédit	La fraude à la paie/au versement
La fraude à la carte présente (Card Present Fraud)	La fraude au prêt
La fraude à la carte non présente (CNP)	**La fraude de première partie**
L’augmentation de la limite de crédit	La fraude au remboursement inhabituel d’un prêt

Le test frauduleux de carte bancaire	**La fraude au prêt actif inhabituel**
Le détournement de carte bancaire	La fraude au compte inactif
La fraude liée à un point d’achat commun (CPP)	L’usurpation d’identité
La fraude au paiement AC (avec carte physique)	La fraude aux paiements ACH frauduleux (fraude par paiement électronique via un réseau Américain)
La fraude par détournement de la paie	

La Problématique de la Détection de la Fraude Bancaire

Il s'agit ici du dispositif de surveillance mis en place pour détecter et prévenir les fraudes sur les transactions et les paiements.

Le principe est que toute activité suspecte doit rapidement faire l'objet d'alerte et être signalée. Ce dispositif repose sur la politique, les procédures, les outils et le facteur humain.

Le Conseil d'Administration adopte une Politique de prévention et de détection de la fraude.
Il met en place des procédures de sécurisation des opérations en amont et en aval, totalement intégrés aux mécanismes de contrôle permanent et de contrôle périodique.

Pour une pleine efficacité, les contrôles manuels ne sont pas recommandés. Il est conseillé de recourir aux systèmes automatisés implémentés, soit à la suite d'acquisition auprès de prestataires externes, soit par développement interne au sein de la banque ou du groupe bancaire lorsque l'expertise existe

<u>Détecter les Fraudes</u> c’est d’abord mettre en place un système combinant le facteur capital humain et la technologie

– des technologies pointues et éprouvées, rapides ayant une grande capacité à enregistrer, stocker et analyser les données

– une base de données complète, avec des indicateurs et des modules pouvant croiser les informations et générer automatiquement les caractéristiques d'une anomalie ou d'une activité anormale, depuis la fraude par piratage de compte à la fraude ACH (utilisation du réseau de transferts électroniques de fonds, prélèvements non autorisés, factures falsifiées, usurpation d'identité, compromission d'email d'entreprise, violation de données sur la base des identifiants bancaires)

– des outils capables de synchroniser la vigilance du Front Office Relation Clientèle avec la surveillance exercée par la Conformité

<u>Prévenir les fraudes</u> en s'appuyant sur la technologie notamment :

– les méthodes d'analyse statistique des données.

- le recours à l'IA via l’exploitation des données (data mining, détecter une fraude bancaire, transactions inhabituelles - montant, pays, type d’achat, connexion à des heures inhabituelles, utilisation soudaine d’un nouveau canal – application, guichet, carte bancaire utilisée à Abidjan puis à Paris 10mn après).

– l'usage de méthodes de pointe pour authentifier, vérifier et identifier les clients et les équipements utilisés (fonctionnalités de biométrie comportementale, empreinte digitale des appareils, chiffrement, authentification bifactorielle).

- La gestion efficiente des flux d'alerte pertinents destinés aux analystes et aux responsables de la conformité (fiche de traitement, rapport périodique d'exploitation, hiérarchiser les nombreux cas de fraude potentiels, et conserver la documentation pour pouvoir l'expliquer aux Auditeurs)

– élargissement de la culture d'entreprise à l'IA et à l'apprentissage automatique.

L'apprentissage automatique est une sous-discipline de l'IA qui consiste à entraîner des modèles à partir des données où les modèles apprennent des exemples pour accomplir une tâche.

En effet, il n'est pas possible d'analyser, de façon manuelle, un volume énorme de données. Il faut des technologies avancées pour regrouper les données.

– redimensionnement de la capacité d'automatisation pour générer les alertes et les rapports d'activité suspects (Suspicious Activity Reports).

Les SAR ne sont pas une preuve de délit, c'est juste un signalement qu'une activité mérite enquête.

Cette approche basée sur le profil de risque de la banque aide la conformité à ne plus perdre du temps à traiter les faux positifs qui sont chronophages.

Le faux positif est une alerte générée sur une activité suspecte, alors qu'il n'y a pas réellement de problème. C'est une alerte déclenchée à tort.

– l'acquisition d'une IA puissante et de logiciels intelligents conçus par des prestataires de solutions de détection de la fraude, qui sont sur le marché.

Ces solutions doivent répondre à un minimum de critères :

– pouvoir intégrer rapidement les données, les flux d'informations négatives dans les médias, les listes de sanctions, les listes des PPE et les bénéficiaires effectifs ultime (UBO - Ultimate Beneficial Owners)…

… personnes physiques qui possèdent ou contrôlent en dernier ressort un compte, une entreprise, une structure ou un montage juridique.

Ce sont eux qui sont *"derrière"* et qui en profitent réellement.

- pouvoir être opérationnels en un mois à deux mois au maximum.

Je vous remercie