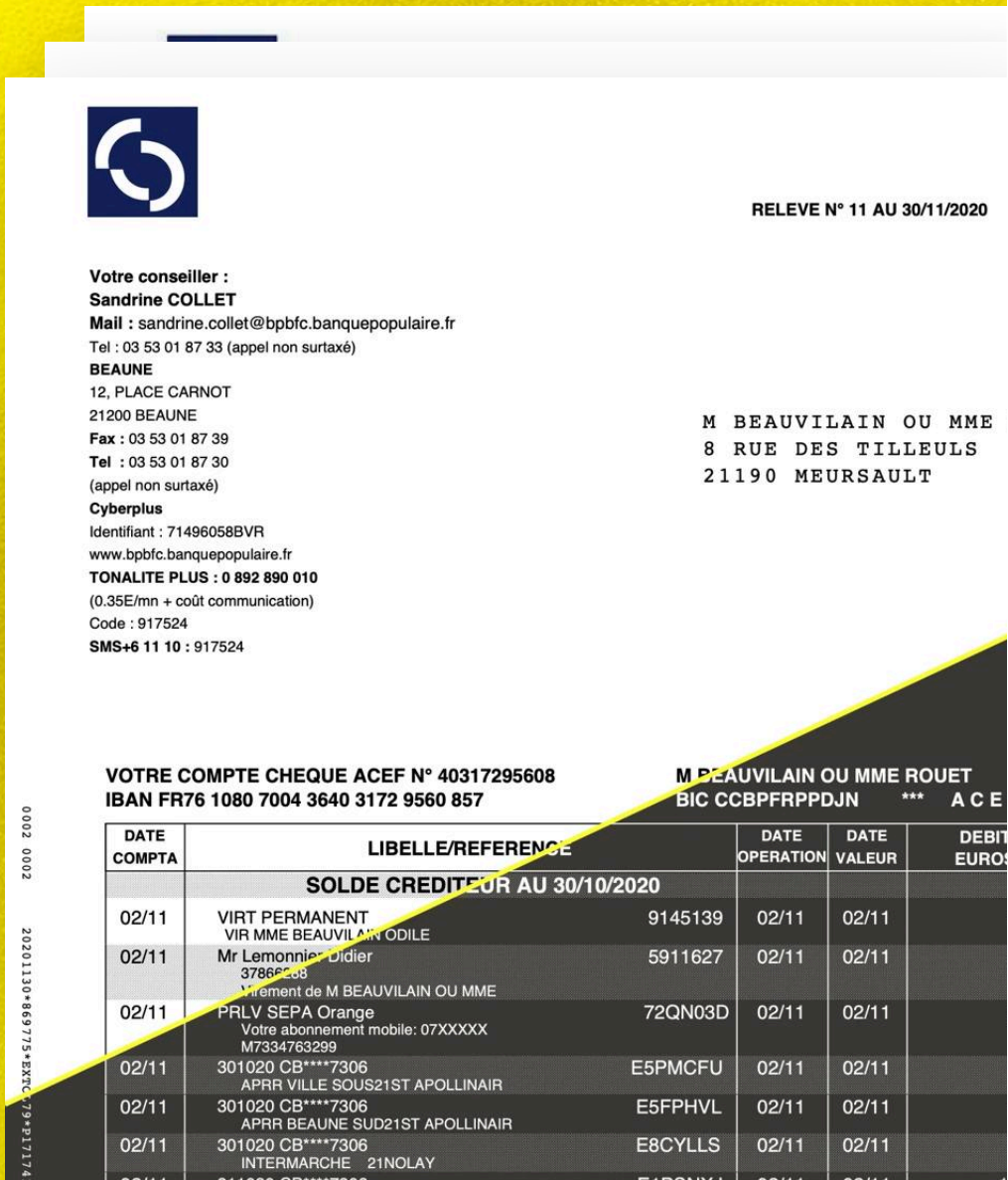
Koncile

Falsification de relevés bancaires : comment détecter les faux IA ?

Assurances, banques et courtiers

Rapport Koncile 2026



RELEVE N° 11 AU 30/11/2020

Votre conseiller :
Sandrine COLLET
Mail : sandrine.collet@bpbfc.banquepopulaire.fr
Tel : 03 53 01 87 33 (appel non surtaxé)
BEAUNE
12, PLACE CARNOT
21200 BEAUNE
Fax : 03 53 01 87 39
Tel : 03 53 01 87 30
(appel non surtaxé)
Cyberplus
Identifiant : 71496058BVR
www.bpbfc.banquepopulaire.fr
TONALITE PLUS : 0 892 890 010
(0.35E/mn + coût communication)
Code : 917524
SMS+6 11 10 : 917524

M BEAUVILAIN OU MME
8 RUE DES TILLEULS
21190 MEURSAULT

VOTRE COMPTE CHEQUE ACEF N° 40317295608
IBAN FR76 1080 7004 3640 3172 9560 857

M BEAUVILAIN OU MME ROUET
BIC CCBPFRPPDJN * A C E**

DATE COMPTA	LIBELLE/REFERENCE		DATE OPERATION	DATE VALEUR	DEBIT EUROS
	SOLDE CREDITEUR AU 30/10/2020				
02/11	VIRT PERMANENT VIR MME BEAUVILAIN ODILE	9145139	02/11	02/11	
02/11	Mr Lemonnier Didier 37866288 Virement de M BEAUVILAIN OU MME	5911627	02/11	02/11	
02/11	PRLV SEPA Orange Votre abonnement mobile: 07XXXXX M7334763299	72QN03D	02/11	02/11	
02/11	301020 CB****7306 APRR VILLE SOUS21ST APOLLINAIR	E5PMCFU	02/11	02/11	
02/11	301020 CB****7306 APRR BEAUNE SUD21ST APOLLINAIR	E5FPHVL	02/11	02/11	
02/11	301020 CB****7306 INTERMARCHE 21NOLAY	E8CYLLS	02/11	02/11	

0002 0002 20201130*869775*EXTC079*F17174

Un workflow complet IA à mettre en place pour lutter contre la fraude

Édito

L'IA fait changer les faux d'échelle

Le constat

Toutes les assurances ont vu défiler de faux fabriqués par IA. La question que tout le monde se pose : est-on armé aujourd'hui pour les détecter ?

Les banques et les courtiers sont dans la même situation avec les relevés bancaires : **85,6 %** des responsables fraude et risque interrogés en 2026 les désignent comme le document le plus vulnérable à la manipulation[1].

Plus de neuf documents modifiés sur dix portent sur des données financières[1], et 17 % des Français connectés déclarent avoir déjà falsifié des documents pour ouvrir un compte ou obtenir un crédit[2]. Les documents signalés comme générés par IA sont **quatre fois plus nombreux** chaque mois en mai 2026 qu'en juin 2025[1]. Le secteur bancaire français a enregistré **plus de 1 milliard d'euros** de pertes en 2023, et l'assurance perd **2,5 milliards d'euros par an**[3].

85,6 %
des responsables fraude et risque jugent le relevé bancaire plus vulnérable que toute autre pièce

La prise de conscience

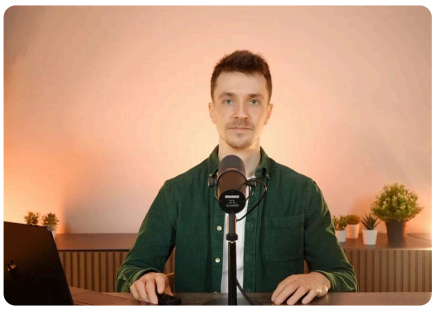
La facilité des outils de falsification est grandissante : la barrière de la technologie a désormais sauté. Les IA sont aussi fortes pour modifier les images que les PDF, parfois sans laisser de trace visible.

Et les IA ne semblent pas aujourd'hui de notre côté : elles sont elles mêmes incapables de détecter leurs propres falsifications. De même, les filtres pour lutter contre la fabrication de faux sont faibles, même chez les acteurs LLM qui affichent un volontarisme pour éviter la falsification[4]. Ils sont aisément contournés par les fraudeurs.

La mise à niveau nécessaire

Les systèmes antifraude doivent être mis à jour pour connaître, anticiper et détecter les comportements des IA. Ce qu'on peut savoir : les IA sont prévisibles. Très souvent, elles vont produire les mêmes traces, utiliser les mêmes outils.

Un mot d'ordre pour les équipes anti-fraude et technologies mises en place : réfléchir comme les fraudeurs pour mieux les détecter. Sur la base de nos recherches en 2026, on a conçu ce livre blanc à la fois pour décrire les **méthodes les plus utilisées** par les fraudeurs aujourd'hui, mais aussi les **4 solutions** efficaces à mettre en place.



Jules Ratier
Cofondateur de Koncile

1. Inscribe, Document Fraud Report 2026. 2. IN BANQUE, Capgemini Invent et Tessi, 2024. 3. Observatoire Tessi 2025 et ALFA. 4. Données Koncile 2026.

Partie 1

Connaître les méthodes des fraudeurs pour mieux y répondre

Grâce à des recueils de données importants et des échanges quotidiens avec des experts des secteurs, nous avons réuni des données uniques sur les principales méthodes utilisées par les falsificateurs. Le phénomène de fraude est toujours constant, mais les formes qu'il prend évoluent. D'où la nécessité d'être toujours à la pointe sur les procédés et intentions des fraudeurs.

Méthode 1 **1** 2 3 4

Les outils de falsification d'images et de PDF, encore omniprésents

Les fraudeurs partent d'un vrai document et le modifient, avec les outils de la suite Adobe ou des outils gratuits qui se trouvent en ligne. Le résultat est crédible à l'œil : un champ est modifié, parfois en gardant exactement la même police de caractères.

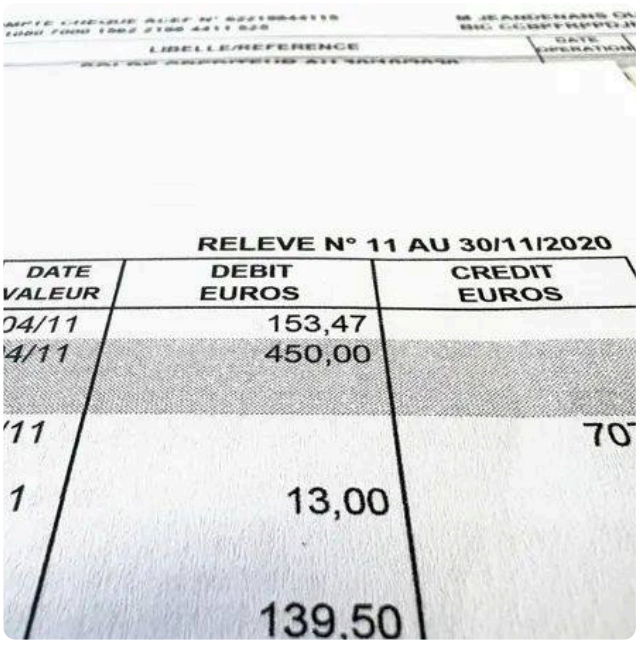
C'est de loin la méthode la plus répandue. Sur un jeu de 150 000 relevés de compte analysés par Koncile, 2 130 étaient falsifiés, et près d'un sur deux sortait d'un simple éditeur de PDF. Sur les photos et les scans, la technique la plus utilisée est le tampon de duplication : on copie une zone propre du document et on la colle sur le chiffre à faire disparaître.

47,6 %
des faux relevés sortent d'un simple éditeur de PDF

Comment la détecter

Sur un PDF, la modification produit souvent une surcouche : au lieu d'être effacées, les données d'origine sont enfouies dans le fichier et peuvent encore être lues. On peut reconstituer le fichier original et le comparer au nouveau.

Sur une image, le tampon laisse des blocs de pixels sensiblement identiques à deux endroits, ou des anomalies de bruit et de compression. Le fichier falsifié est souvent imprimé puis rescanné pour effacer ces traces.



Une photo de relevé prise au téléphone : chaque chiffre se retouche comme un pixel.

Méthode 2 1 **2** 3 4

Altérations par IA, la nouvelle donne 2026

Les faux faits par IA restent minoritaires, mais ils sont en forte accélération cette année. On l'a vu sur de faux tickets de caisse ou des cartes d'identité modifiées. Les modèles d'image savent régénérer un document entier, ou ne réécrire qu'une zone, un montant ou un nom, en respectant la police et le grain du reste.

Les assistants ont des filtres : ils refusent le plus souvent de produire un faux quand c'est clairement demandé. Le résultat est parfois caricatural. Mais souvent, il est complètement invisible à l'œil nu. Nos mesures portent sur 5 244 faux issus de 56 modèles d'image.

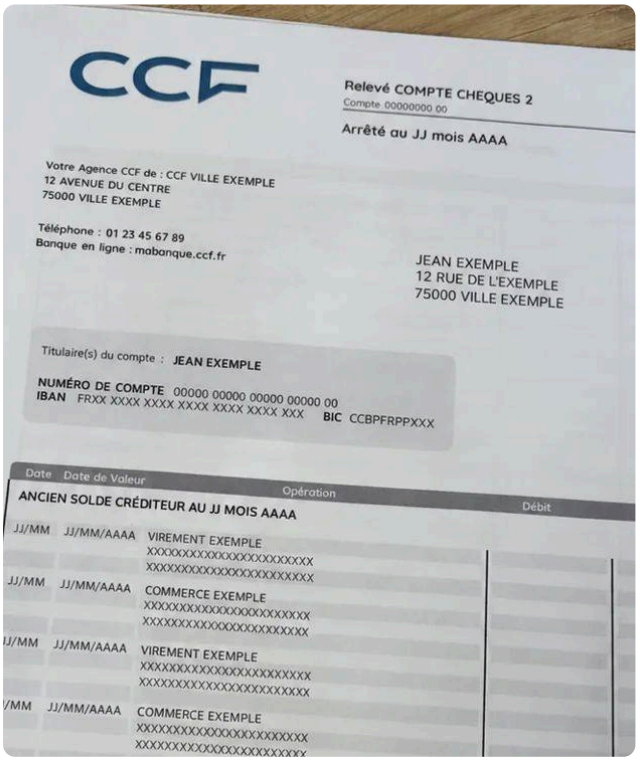
0,039 $

coût médian d'un faux fabriqué par un modèle d'image

Comment la détecter

Il reste deux types de traces. Une mention dans les métadonnées, qui dit que l'image a été générée par une IA, mais qu'un fraudeur peut effacer. Et un filigrane invisible dans les pixels, que chaque laboratoire applique à sa façon, quand il l'applique.

Les IA reconnaissent d'ailleurs assez mal une image générée, même par elles. Le plus fiable reste un modèle entraîné sur de vrais documents et sur leurs versions générées ou modifiées. La retouche d'un seul champ, elle, reste très difficile à détecter par l'image seule : ce sont les contrôles de cohérence qui prennent le relais.


CCF

Relevé COMPTE CHEQUES 2
Compte 00000000 00
Arrêté au JJ mois AAAA

Votre Agence CCF de : CCF VILLE EXEMPLE
12 AVENUE DU CENTRE
75000 VILLE EXEMPLE

Téléphone : 01 23 45 67 89
Banque en ligne : mabanque.ccf.fr

JEAN EXEMPLE
12 RUE DE L'EXEMPLE
75000 VILLE EXEMPLE

Titulaire(s) du compte : JEAN EXEMPLE

NUMÉRO DE COMPTE 00000 00000 00000 00000 00
IBAN FRXX XXXX XXXX XXXX XXXX XXXX XXX BIC CCBPFRPPXXX

Date	Date de Valeur	Opération	Débit
		ANCIEN SOLDE CRÉDITEUR AU JJ MOIS AAAA	
JJ/MM	JJ/MM/AAAA	VIREMENT EXEMPLE XXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXX	
JJ/MM	JJ/MM/AAAA	COMMERCE EXEMPLE XXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXX	
JJ/MM	JJ/MM/AAAA	VIREMENT EXEMPLE XXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXX	
/MM	JJ/MM/AAAA	COMMERCE EXEMPLE XXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXX	

Un relevé d'exemple, données fictives, tel qu'un modèle d'image sait le produire.

Méthode 3 1 2 **3** 4

Agent IA et fichiers natifs : des traces sont systématiquement laissées

Un assistant capable d'exécuter du code ouvre le PDF de la banque, remplace un montant et réenregistre le fichier. Le résultat est visuellement parfait, mais l'outil signe son passage.

Il ne dessine rien : il écrit un petit programme qui ouvre le fichier avec une bibliothèque PDF de bas niveau, change une valeur et le réenregistre. Dans nos essais, la plupart des assistants refusent de falsifier un montant, mais 9 modèles sur 14 acceptent « d'anonymiser » un document.

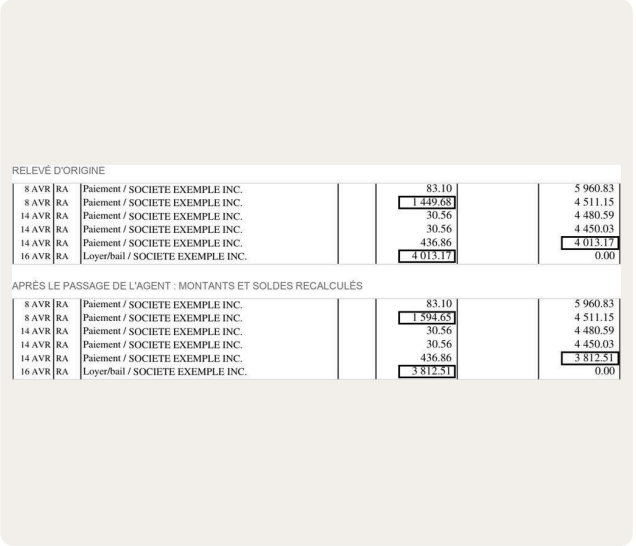
72 %

des agents utilisent la même de modification bibliothèque, pikepdf, selon notre étude

Comment la détecter

Aucune banque n'émet ses relevés avec ces bibliothèques. Elles laissent une signature en clair dans le fichier, un style d'écriture qui leur est propre et un niveau de compression particulier.

Attention, certaines conservent les métadonnées d'origine : un simple détecteur de métadonnées passe à côté. Et dans 39 % des cas, l'ancienne valeur subsiste ailleurs dans le fichier.


RELEVÉ D'ORIGINE

8 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	83.10	5 960.83
8 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	1 449.68	4 511.15
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	30.56	4 480.59
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	30.56	4 450.03
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	436.86	4 013.17
16 AVR	RA	Loyer/bail / SOCIETE EXEMPLE INC.	4 013.17	0.00

APRÈS LE PASSAGE DE L'AGENT : MONTANTS ET SOLDES RECALCULÉS

8 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	83.10	5 960.83
8 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	1 594.65	4 511.15
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	30.56	4 480.59
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	30.56	4 450.03
14 AVR	RA	Paiement / SOCIETE EXEMPLE INC.	436.86	3 812.51
16 AVR	RA	Loyer/bail / SOCIETE EXEMPLE INC.	3 812.51	0.00

Un relevé d'exemple avant puis après le passage d'un agent.

Méthode 4 1 2 3 **4**

Des templates farms, toujours aussi actives

Une template farm, c'est une grosse bibliothèque, un grand supermarché de documents vierges. Le fraudeur choisit une banque dans un catalogue, remplit un formulaire en ligne (nom, adresse, solde, lignes d'opérations) et télécharge le fichier. À l'écran, le résultat est propre.

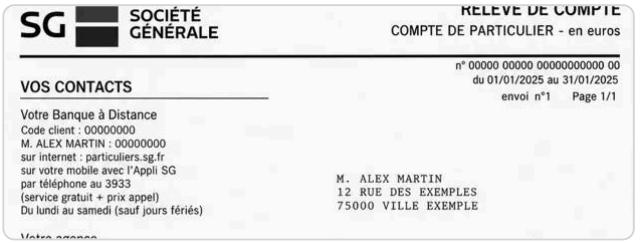
Parmi les relevés falsifiés de notre base, 18,9 % sortaient d'une de ces bibliothèques, et nous en avons identifié plusieurs dizaines. Elles ne demandent aucune compétence, coûtent quelques euros et réapparaissent plus vite qu'elles ne ferment.

18,9 %
des faux relevés sortent d'une template farm

Comment la détecter

Ces générations laissent toujours de multiples traces, en particulier dans les métadonnées du fichier. Mais les métadonnées restent une information déclarée par le fichier, un peu comme une étiquette sur un produit, qui peut ne pas refléter la réalité : certains outils les maquillent.

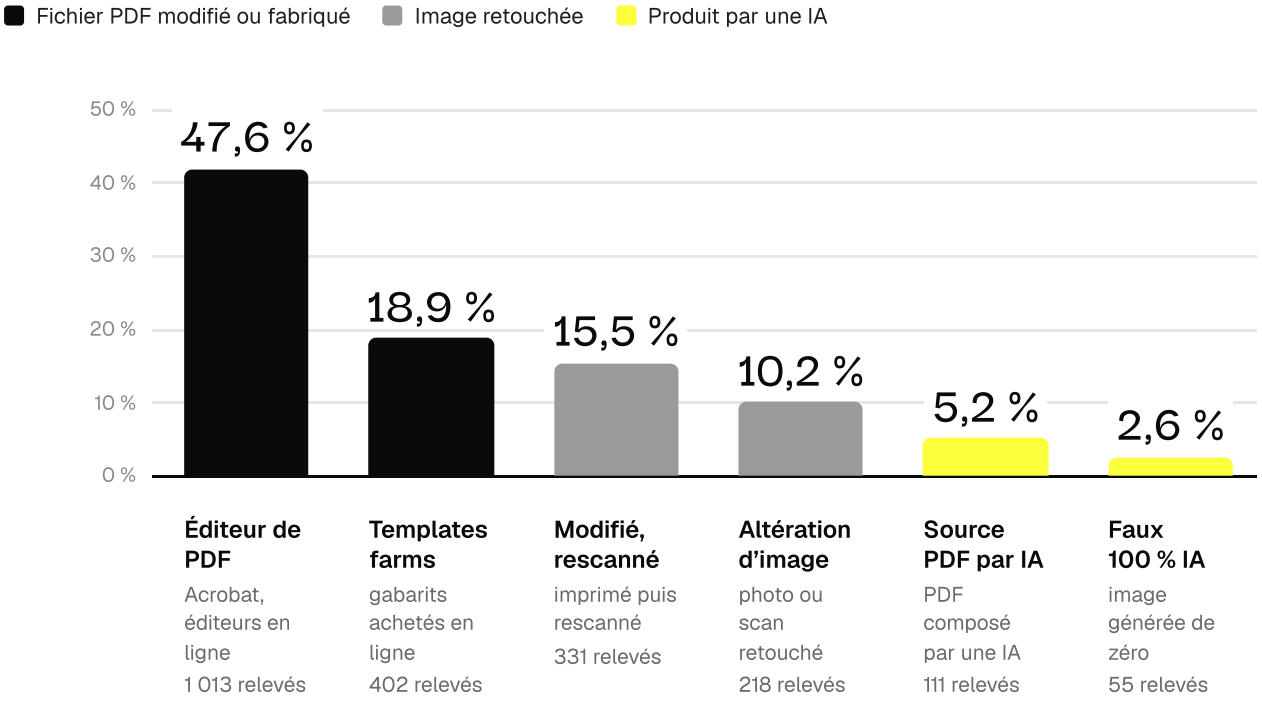
Reste la chaîne d'émission d'une banque, qu'un gabarit ne reproduit jamais entièrement. Les faux d'un même gabarit se ressemblent entre eux, jusqu'aux mêmes défauts.


SG SOCIÉTÉ GÉNÉRALE
RELEVÉ DE COMPTE
COMPTE DE PARTICULIER - en euros
n° 00000 00000 00000000000 00
du 01/01/2025 au 31/01/2025
envoi n°1 Page 1/1
VOS CONTACTS
Votre Banque à Distance
Code client : 00000000
M. ALEX MARTIN : 00000000
sur internet : particuliers.sg.fr
sur votre mobile avec l'Appli SG
par téléphone au 3933
(service gratuit + prix appel)
Du lundi au samedi (sauf jours fériés)
M. ALEX MARTIN
12 RUE DES EXEMPLES
75000 VILLE EXEMPLE

Un relevé spécimen, données fictives : c'est cette mise en page que les gabarits reproduisent.

Comment sont fabriqués les faux relevés

Part de chaque mode opératoire parmi les relevés falsifiés. Source : Koncile.



Cas d'étude

OnlyFake : la chute d'une industrie du faux

La chute

En février 2026, Yurii Nazarenko, un Ukrainien de 27 ans, est jugé à New York. C'est le créateur d'OnlyFake. Ce site a fabriqué des milliers de photos de faux documents entre 2021 et 2024 : faux permis de conduire, faux passeports, fausses cartes de sécurité sociale. Il était accessible au grand public, et il était très facile d'y obtenir une photo réaliste d'un faux document.

Extradé de Roumanie vers les États-Unis en septembre 2025, il a plaidé coupable et accepté de restituer 1,2 million de dollars, l'équivalent des recettes du site. Sur des forums, le service affichait des captures de comptes ouverts avec ses faux dans plus de 120 sociétés : plateformes de cryptomonnaies, néobanques, services de paiement, sites de paris.

1,2 M$
restitués par le créateur d'OnlyFake

120+
sociétés visées par les faux du service

La reprise

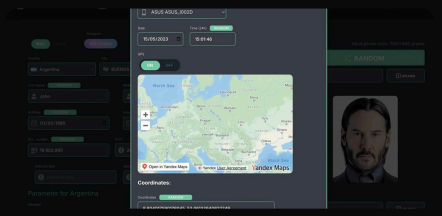
L'histoire ne s'arrête pas là. Un site, MacDoc, reprend OnlyFake presque tel quel : accessible depuis Google et non sur le darknet, il vend la photo d'un faux passeport ou d'une fausse carte d'identité à partir de 15 euros, payés en cryptomonnaie. Le pseudo contrat du nouveau site porte encore l'ancien nom.



Spécimen de faux passeport produit par le site.

Pas d'IA, des calques

L'utilisateur remplit un formulaire. Les champs sont posés en calques sur une image de document, puis des filtres de flou et de grain donnent un aspect photographique : la carte posée sur une table ou sur un tissu, pour faire réaliste. L'outil calcule de fausses bandes MRZ et simule la marque du téléphone, l'horodatage et la position GPS de la photo.



L'écran qui fabrique de fausses métadonnées : appareil, date, position GPS.

Ce qui le trahit

Ces photos laissent beaucoup de traces. Sur une fausse carte d'identité française, nous avons relevé 5 erreurs de typographie et de positionnement, visibles à l'œil nu. Le format des adresses, saisi librement, est très souvent erroné. Les métadonnées simulées sont très imparfaites, et un code 2D-Doc ne se recrée pas sans la clé privée de l'administration.

Les justificatifs financiers suivent la même logique de fabrication : un formulaire, un gabarit, un habillage. L'analyse complète est publiée sur koncile.ai.

Partie 2

La riposte : identifier les outils, méthodes et technologies efficaces en 2026

Aucune technologie ne suffit seule. Quatre méthodes se complètent, chacune avec ce qu'elle voit et ce qui lui échappe. Chaque contrôle apporte sa contribution à un score de fraude global, et c'est ce score qui décide, pas un test isolé.

Méthode de détection 1 1 2 3 4

Analyse forensics traditionnelle : le 80/20

C'est la technologie la plus abordable, et celle qui détecte la plupart des fautes : lire le fichier lui même, pas seulement ce qu'il affiche.

Lire les métadonnées

Chaque PDF déclare le logiciel qui l'a créé et celui qui l'a enregistré, avec ses dates. Beaucoup de fraudeurs les laissent en clair. Un relevé au nom d'une banque écrit par Word, Canva ou un éditeur de PDF est une alerte.

Ces champs se modifient facilement. Mais la façon dont les objets sont écrits, compressés et enchaînés trahit l'outil qui a réellement produit le fichier. Un fraudeur maquille les métadonnées, il ne réécrit pas le style d'écriture de son éditeur.

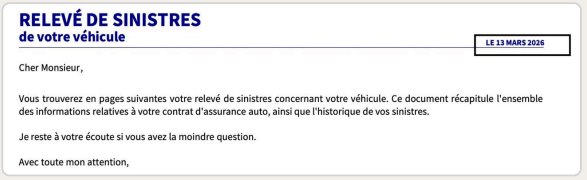
1 sur 150
fichiers garde la trace d'une modification, en production

Identifier les traces du fichier antérieur

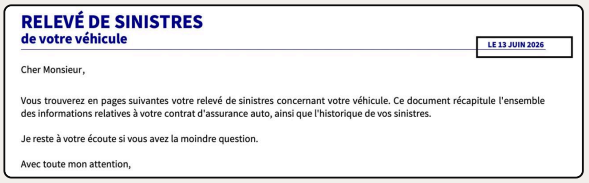
Quand un éditeur modifie un PDF sans le réécrire, il ajoute une couche en fin de fichier : on retrouve alors la valeur d'origine. Une police intégrée autrement que les autres est souvent celle qu'un éditeur a ajoutée pour réécrire un montant.

Exemple : un relevé modifié, avant et après

Avant, la version d'origine retrouvée dans le fichier


RELEVÉ DE SINISTRES
de votre véhicule
LE 13 MARS 2026
Cher Monsieur,
Vous trouverez en pages suivantes votre relevé de sinistres concernant votre véhicule. Ce document récapitule l'ensemble des informations relatives à votre contrat d'assurance auto, ainsi que l'historique de vos sinistres.
Je reste à votre écoute si vous avez la moindre question.
Avec toute mon attention,

Après la version présentée : la date est passée du 13 mars au 13 juin 2026


RELEVÉ DE SINISTRES
de votre véhicule
LE 13 JUIN 2026
Cher Monsieur,
Vous trouverez en pages suivantes votre relevé de sinistres concernant votre véhicule. Ce document récapitule l'ensemble des informations relatives à votre contrat d'assurance auto, ainsi que l'historique de vos sinistres.
Je reste à votre écoute si vous avez la moindre question.
Avec toute mon attention,

Autre cas : un rectangle blanc posé sur un montant, puis réécrit par dessus. Nous en avons trouvé 3 sur 1 340 PDF analysés, sans aucune fausse alerte.

Les pièges

Un réenregistrement sur l'ordinateur du client change l'outil sans qu'il y ait fraude. Plusieurs justificatifs passent par un outil d'assemblage sans qu'aucune page ne soit modifiée. Sans calibration, un test de métadonnées produit 10 à 20 % de fausses alertes.


CE QUI S'AFFICHE

• SINISTRES DECLARES AU COURS DES 5 DERNIERES ANNEES AU 01/01/2019

Numéro	Date	Responsabilité	Conducteur
NEANT			

CE QUI RESTE SOUS LES CACHES BLANCS

• SINISTRES DECLARES AU COURS DES 5 DERNIERES ANNEES AU 01/01/2019

Numéro	Date	Responsabilité	Conducteur
A1231234	19.04.2014	TOTALE	CONDUCTEUR 3
A1231235	06.03.2014	AUCUNE	CONDUCTEUR 2

Le document affiche « Néant » ; sous les caches blancs, deux sinistres sont toujours dans le fichier.

Méthode de détection 2 1 **2** 3 4

Machine learning : le passage obligé pour les photos altérées par l'IA

Quand la retouche est faite par un modèle d'image, rien ne se lit dans le fichier. Il faut un modèle entraîné à reconnaître ce que les générateurs laissent dans les pixels.

Pour détecter une altération d'image, il faut passer par du machine learning : un assistant généraliste ne voit pas ces retouches. Entraîné sur de vrais documents et sur leurs versions générées ou retouchées, le modèle donne un score par zone de l'image et montre les zones suspectes.

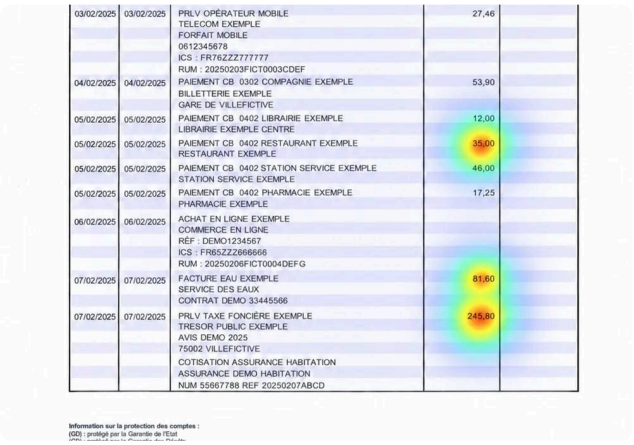
92 %

des faux détectés par un modèle spécialisé, contre 56 % pour le meilleur assistant généraliste

Ce sont les données qui font le modèle. Les détecteurs publics d'images IA, sans entraînement sur des documents, répondent presque au hasard : 50 à 62 % dans nos essais. Réentraînés sur des documents, ils dépassent 90 %.

Un système en deux temps

Le modèle trouve des zones suspectes, il ne sait pas si elles comptent. Une seconde lecture juge si la zone vaut la peine d'être modifiée : un montant, un nom, une date. C'est là que la fraude est identifiée.



03/02/2025	03/02/2025	PRLV OPÉRATEUR MOBILE TELECOM EXEMPLE FORFAIT MOBILE 0612345678 ICS : FR76ZZZ7777777 RUM : 20250203FICT0003CDEF	27,46
04/02/2025	04/02/2025	PAIEMENT CB 0302 COMPAGNIE EXEMPLE BILLETTERIE EXEMPLE GARE DE VILLEFICTIVE	53,90
05/02/2025	05/02/2025	PAIEMENT CB 0402 LIBRAIRIE EXEMPLE LIBRAIRIE EXEMPLE CENTRE	12,00
05/02/2025	05/02/2025	PAIEMENT CB 0402 RESTAURANT EXEMPLE RESTAURANT EXEMPLE	35,00
05/02/2025	05/02/2025	PAIEMENT CB 0402 STATION SERVICE EXEMPLE STATION SERVICE EXEMPLE	46,00
05/02/2025	05/02/2025	PAIEMENT CB 0402 PHARMACIE EXEMPLE PHARMACIE EXEMPLE	17,25
06/02/2025	06/02/2025	ACHAT EN LIGNE EXEMPLE COMMERCE EN LIGNE RÉF : DEMO1234567 ICS : FR65ZZZ666666 RUM : 20250206FICT0004DEFG	
07/02/2025	07/02/2025	FACTURE EAU EXEMPLE SERVICE DES EAUX CONTRAT DEMO 33445566	81,60
07/02/2025	07/02/2025	PRLV TAXE FONCIÈRE EXEMPLE TRESOR PUBLIC EXEMPLE AVIS DEMO 2025 75002 VILLEFICTIVE	245,80
		COTISATION ASSURANCE HABITATION ASSURANCE DEMO HABITATION NUM 55667788 REF 20250207ABCD	

Sur ce relevé d'exemple, le modèle désigne les montants retouchés.

Ses limites

La retouche d'un seul champ par une IA, un faux réenregistré dans un autre format, et tout ce qui n'est pas une image : le modèle ne lit pas les fichiers natifs. Il faut aussi des données du bon type : un modèle qui reconnaît un faux ticket de caisse ne reconnaîtra pas forcément une fausse fiche de paie.

Méthode de détection 3 1 2 **3** 4

La base de connaissance des fichiers : le rempart contre les meilleurs fraudeurs

Chaque banque produit ses relevés avec sa propre chaîne logicielle. Confronter un fichier aux relevés authentiques du même émetteur révèle le faux le plus soigné.

Pour chaque banque, on mémorise à quoi ressemble un relevé tel qu'il sort de sa chaîne d'émission. Pas seulement les logiciels déclarés : une cinquantaine de traces informatiques, comme le chiffrement, la compression, la structure des pages ou la façon dont les polices sont intégrées.

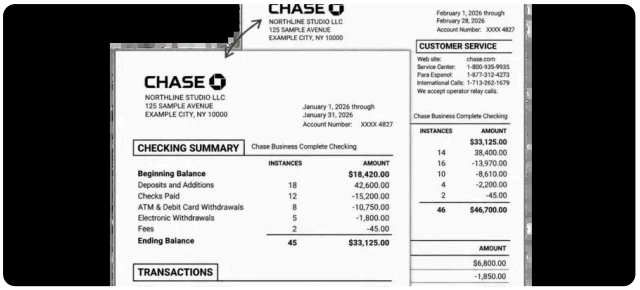
140+

banques reconnues, et la base grandit à chaque relevé

Un relevé authentique de la même banque reproduit ce profil à l'identique. Un faux, même soigné, s'en écarte presque toujours sur un point, et chaque écart devient un signal. À l'inverse, un émetteur authentique qui utilise un outil inhabituel cesse d'être signalé à tort.

Pourquoi c'est un rempart

Une retouche touche presque toujours l'enveloppe du fichier, parce que l'outil qui retouche réécrit le fichier à sa façon. Imiter l'empreinte exacte d'une banque suppose de connaître toute sa chaîne de production.



Deux relevés d'exemple du même émetteur, données fictives : même empreinte attendue.

Sa limite

Il faut des relevés authentiques de chaque émetteur, et un enrichissement permanent. Le profil d'un fichier ne vaut que pour les fichiers natifs : un scan ou une photo viennent du client, pas de la banque.

Méthode de détection 4 1 2 3 **4**

Contrôles contextuels : simples mais efficaces

Un faux doit rester cohérent avec lui même et avec le monde réel. Ces contrôles ne regardent ni le fichier ni l'image : ils vérifient ce que le document dit.

Les sommes et le détail des lignes

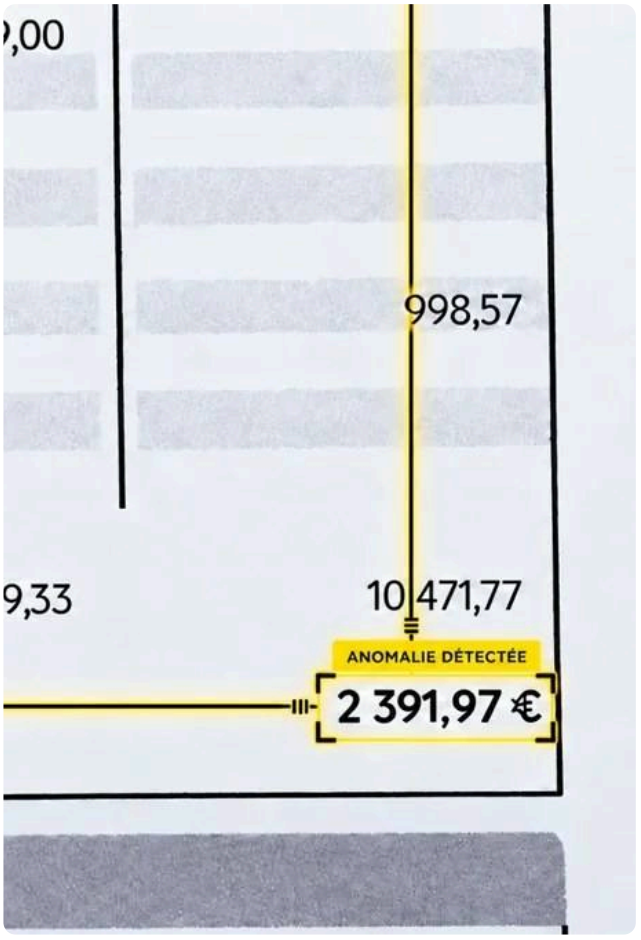
Additionner les lignes au débit et au crédit, puis comparer aux totaux calculés par la banque. Le fraudeur a parfois oublié de mettre à jour tout le relevé. Sur un relevé falsifié, les 450 euros affichés au débit ne correspondaient pas aux 505,89 euros de capital détaillés dans le libellé.

36
relevés de notre base attribués à un tiers par simple changement de titulaire

Le titulaire, l'IBAN, le 2D-Doc

Une personne s'attribue le relevé d'un tiers en remplaçant le nom, et toutes les lignes restent cohérentes entre elles. Pour une société, on croise avec le registre du commerce. L'IBAN révèle l'identité de la banque, et se recoupe avec le relevé.

Sur les justificatifs qui en portent un, le 2D-Doc contient les valeurs clés du document, signées par l'émetteur. Il faut comparer les valeurs lues dans le code avec celles imprimées : un fraudeur peut recopier un code authentique sur un document dont il a changé les chiffres.



Sur ce relevé d'exemple, le solde final ne correspond pas à la somme des opérations.

Leur limite

Une partie des faux passe sans difficulté : il suffit au fraudeur d'avoir recalculé les soldes. Et une seule erreur de lecture du document peut produire une fausse alerte.

80/100

Un signal, pas une accusation

On ne sait jamais avec certitude qu'un relevé est modifié : on mesure un risque. Le résultat est un score de 0 à 100, avec un risque élevé à partir de 80. La décision revient toujours à une personne.



Entretien

« Vérifier une pièce à la main, c'est du temps que mes équipes ne passent pas avec nos clients. »

Ghislain Averty

Directeur des opérations et de l'actuariat, AND-E, assureur de la marque Toyota Assurances

Toyota Assurances

Chez Toyota Assurances, les équipes vérifiaient à la main chaque carte grise, chaque permis, chaque relevé d'information. En quatre mois, de zéro à la production, la lecture des pièces de souscription a été automatisée. Ghislain Averty raconte ce que ses équipes font du temps libéré, et où en est la détection de fraude.

60 000
polices automobiles en portefeuille

70 %
de temps gagné sur le contrôle des pièces

95 à 99 %
des données lues automatiquement

3 à 4 ETP
libérés et réaffectés à la rétention

Qu'est ce qui vous a décidé à automatiser ?

Pour moi, l'intelligence des gestionnaires et des souscripteurs doit être utilisée à autre chose : rappeler un client pour le retenir, comprendre pourquoi il veut résilier, essayer de trouver des solutions avec lui, plutôt que passer du temps à regarder une donnée et vérifier que c'est la bonne, alors que cela peut être automatisé.

Il s'agit d'utiliser l'intelligence humaine pour des relations humaines, et non pour des tâches de robot. Contrôler une donnée, la lire, la retrouver, puis la vérifier : c'est un temps infini. Et nos volumes augmentent.

Quels gains mesurez vous aujourd'hui ?

À trois mois à peine de l'installation, je pense que nous avons gagné environ 70 % du temps que nous passions à contrôler les pièces. C'est énorme, en temps et en argent. Par rapport à la taille de notre entreprise, sur cette tâche précise, je dirais que nous avons gagné environ trois à quatre ETP.

Et la détection de fraude ?

Nous n'y sommes pas encore : ce sera une étape ultérieure. La priorité immédiate était d'optimiser les process. Dans un second temps, nous travaillerons la fraude documentaire. Sur notre propre activité liée à Toyota et Lexus, compte tenu de la façon dont nous sélectionnons et acquérons nos clients, il y a très peu de fraude. En automobile en général, il y en a beaucoup, c'est clair, notamment via les comparateurs.

À qui recommanderiez vous la démarche ?

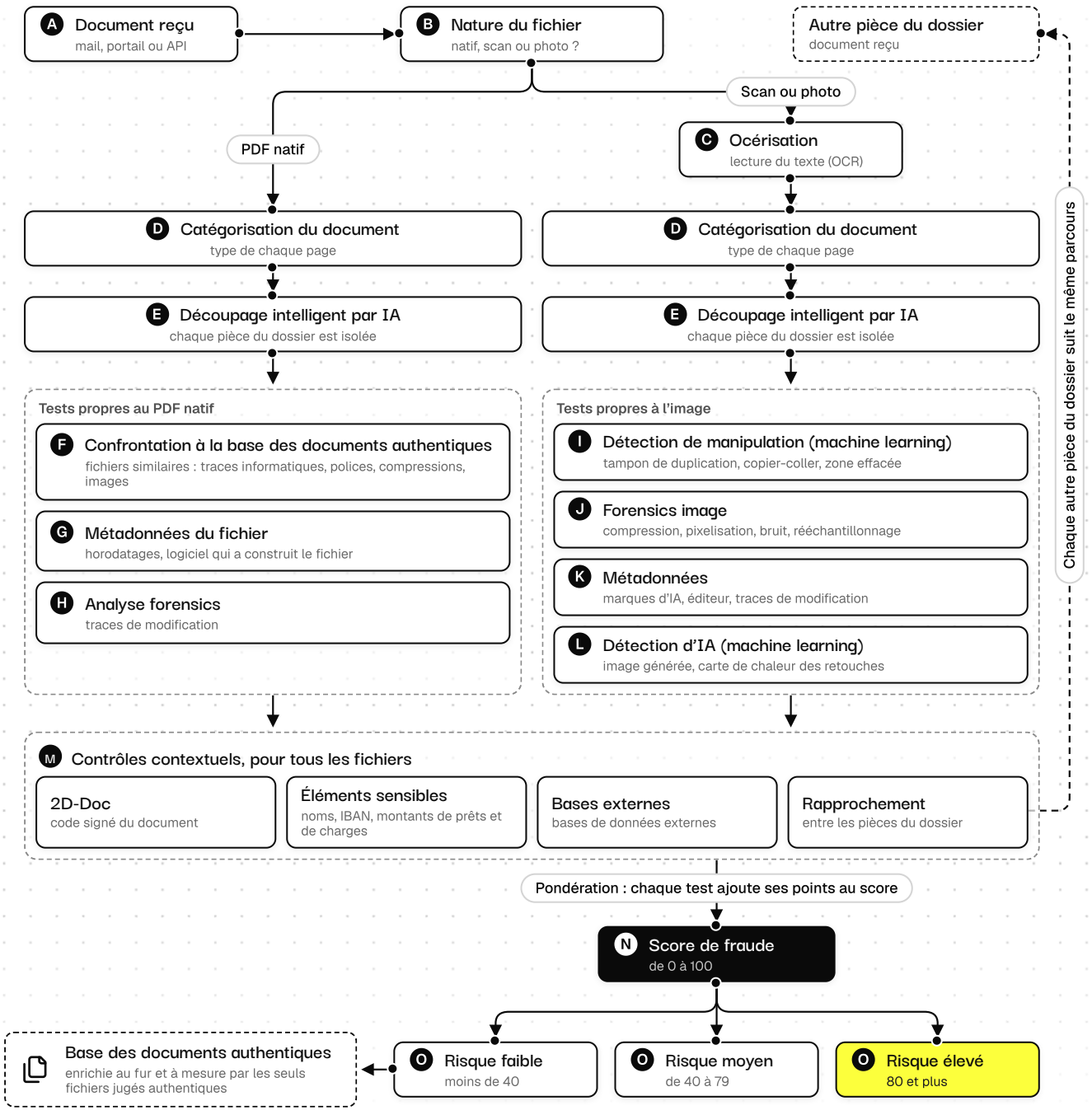
Surtout aux courtiers en assurance, et aux assureurs aussi. Koncile est une entreprise à taille humaine, avec qui il a été facile de travailler, notamment pour nos équipes informatiques. Il y a de la dynamique. Et ceux qui ne se sont pas encore mis à l'OCR, j'en connais beaucoup, courtiers, courtiers grossistes ou assureurs : il n'y a aucune raison de freiner cela, et c'est beaucoup moins cher que ce qu'on imagine.

Entretien réalisé en vidéo par Tristan Thommen, cofondateur de Koncile, le 1er septembre 2026. Propos édités pour la lecture.

Le workflow

Un workflow IA auto-apprenant conçu pour détecter la fraude

Détecter la fraude demande de mettre en place tout un mécanisme : du traitement de documents (document processing) et une combinaison d'outils qui, mis ensemble, permettent d'apprécier la fraude. Car la fraude est toujours un faisceau d'indices. Pour minimiser les faux positifs, il faut bâtir un score, et ce score s'appuie sur une combinaison d'indices. Tout l'enjeu est d'arriver à la bonne pondération.



Le workflow

Chaque étape expliquée

Chaque lettre renvoie à une étape du schéma de la page précédente.

A Document reçu

Le document arrive par mail, par un portail ou par API. On analyse le fichier tel qu'il a été reçu, pas une copie réenregistrée : un fichier d'origine garde bien plus de traces.

B Nature du fichier

C'est toujours la première étape : PDF natif, ou scan et photo ? La réponse oriente toute la suite, car les tests de fraude sont propres à l'un ou à l'autre. Un document ne suit qu'un seul des deux couloirs.

C Océrisation

Un scan ou une photo n'est qu'une image. L'océrisation (OCR) en lit le texte et les données, champ par champ, pour que la suite du parcours soit la même que pour un fichier natif.

D Catégorisation du document

Chaque page reçoit un type : relevé de compte, pièce d'identité, fiche de paie, justificatif de domicile. Le type décide des contrôles qui s'appliqueront.

E Découpage intelligent par IA

Un dossier arrive souvent en un seul fichier qui contient plusieurs pièces. L'IA détermine où commence et où finit chacune, pour qu'elle soit analysée séparément.

F Confrontation à la base des documents authentiques

Uniquement pour les PDF natifs, et c'est une étape clé : toutes les traces informatiques du fichier, ses polices, ses compressions, ses images, sont confrontées à celles des fichiers similaires déjà connus comme authentiques. La base s'enrichit au fur et à mesure, pour tous les émetteurs de relevés de compte, avec les seuls fichiers jugés authentiques.

G Métadonnées du fichier

Les métadonnées générales du PDF : les horodatages, et qui a construit le fichier, c'est à dire le logiciel qui l'a produit.

H Analyse forensics

On lit la structure du fichier : les couches ajoutées après coup, l'ancienne valeur restée sous la nouvelle.

I Détection de manipulation (machine learning)

Des modèles de machine learning cherchent les gestes de retouche : tampon de duplication (clone stamp), zone copiée puis collée, élément effacé. Des modèles publics issus de la recherche existent, comme TruFor, CAT-Net, Noiseprint ou DocTamper.

J Forensics image

On analyse la matière de l'image, sans modèle : niveaux de compression et zones compressées deux fois, pixelisation, bruit qui change d'un endroit à l'autre, traces de rééchantillonnage.

K Métadonnées

Deux lectures. Les métadonnées d'IA, c'est à dire les marques laissées par les générateurs d'images. Et les métadonnées classiques du fichier, pour repérer une trace de modification ou un éditeur inhabituel.

L Détection d'IA (machine learning)

Un modèle de machine learning en deux parties. La première reconnaît les images entièrement générées. La seconde dessine une carte de chaleur (heatmap) pour un cas plus subtil : le fichier modifié en partie par IA. Là aussi, des modèles publics existent, comme Community Forensics ou NPR.

M Contrôles contextuels

Pour une image comme pour un fichier natif : le 2D-Doc, le contrôle des montants, la confrontation à des bases de données externes. L'attention se porte sur les éléments les plus falsifiés : les noms, les IBAN, les montants sensibles comme les prêts et les charges. C'est aussi ici que les pièces du dossier, qui ont chacune suivi leur parcours, sont rapprochées entre elles.

N Score de fraude

Chaque test ajoute des points à un score de 0 à 100 selon sa pondération, avec la raison de chaque signal. C'est le score qui décide, pas un test isolé.

O La décision

Sous 40, le risque est faible. De 40 à 79, il est moyen. À partir de 80, il est élevé et le dossier est revu par une personne. Un score reste un signal à vérifier, jamais une accusation.

Ils nous font confiance

Assurance, banque, finance et grands groupes



































Jules Ratier

Cofondateur

jules@koncile.ai



Tristan Thommen

Cofondateur et CTO

tristan@koncile.ai

Koncile

Document processing and fraud detection

2 rue de Lancry, 75010 Paris

+33 9 75 86 62 90

www.koncile.ai