

Meilleures pratiques pour lutter contre les arnaques dans la publicité - ICC / GASA



© Juin 2026 - International Chamber of Commerce (ICC) / Global Anti Scams Alliance (GASA)
Traduction ARPP

L'International Chamber of Commerce et la Global Anti Scams Alliance détiennent tous les droits de propriété intellectuelle sur cet ouvrage collectif et encouragent sa reproduction et sa diffusion sous réserve des conditions suivantes :

- Les organisations autrices doivent être citées comme source et détentrices des droits d'auteur, en mentionnant le titre du document, © International Chamber of Commerce / Global Anti Scams Alliance, ainsi que l'année de publication.
- Une autorisation écrite expresse doit être obtenue pour toute modification, adaptation ou traduction, pour toute utilisation commerciale, et pour toute utilisation susceptible de laisser entendre qu'une autre organisation ou personne est à l'origine du travail ou y est associée.
- L'ouvrage ne peut être reproduit ou mis à disposition sur des sites web, sauf par le biais d'un lien vers la page web ICC pertinente (et non vers le document lui-même). Les demandes d'autorisation peuvent être adressées à l'ICC via l'adresse suivante : ipmanagement@iccwbo.org.

Table des matières

I. Introduction et contexte.....	4
II. Principes clés pour lutter contre la publicité frauduleuse.....	7
III. Bonnes pratiques pour les plateformes, les agences et autres acteurs afin de lutter contre les arnaques.....	10
A. Systèmes de vérification progressive basés sur le risque.....	10
B. Fonctionnalités complémentaires de sécurité par conception.....	15
C. Renforcer la transparence et le contrôle utilisateur.....	18
D. Participation au partage de signaux d’arnaque et de renseignements.....	20
IV. Collaboration pour renforcer la défense collective.....	21

I. Introduction et contexte

Le défi des arnaques publicitaires

Une étude récente de la **Global Anti-Scam Alliance (GASA)** estime que les arnaques coûtent **442 milliards de dollars par an** aux particuliers et aux entreprises dans le monde.¹ Les arnaques nuisent aux consommateurs comme aux entreprises légitimes. Les escroqueries en ligne constituent un problème mondial croissant, touchant des personnes de tous âges et de tous horizons.² L'utilisation par les escrocs d'infrastructures numériques, y compris la publicité en ligne, saper la confiance des utilisateurs dans les écosystèmes numériques et publicitaires, engendre des coûts économiques considérables et porte préjudice aux individus et aux communautés à l'échelle mondiale.

Les fraudeurs ne cessent de faire évoluer leurs tactiques et de tirer parti des nouvelles technologies et tendances sociales. La convergence de la publicité ciblée pilotée par l'intelligence artificielle (IA), des systèmes de paiement automatisés, des technologies d'anonymisation et des réseaux mondiaux a créé un écosystème criminel complexe qui transcende les frontières. Les fraudeurs déguisent des contenus illicites en publicités en ligne légitimes ou attirent les victimes via des liens hors plateforme, tandis que les paiements sont traités par des serveurs à l'étranger, ce qui rend le traçage et la répression un défi permanent.

Les risques liés aux arnaques dans la publicité ne doivent pas être interprétés de manière étroite. De plus en plus, les activités frauduleuses émergent au sein d'un écosystème transplateforme plus large dans lequel des contenus payants trompeurs, des promotions de type influenceur, l'usurpation d'identité, les applications de messagerie et les incitations financières ou liées aux cryptomonnaies peuvent interagir dans le cadre d'un même parcours d'arnaque. Dans de nombreux cas, la publicité n'est pas le point final du préjudice, mais le point d'entrée d'une chaîne de manipulation plus large qui peut rapidement amener les utilisateurs vers des environnements hors plateforme, où la répression devient plus difficile.

L'ampleur du défi est également façonnée par le volume et la diversité des annonceurs opérant en ligne. La grande majorité d'entre eux – petites entreprises, travailleurs indépendants et

¹ GASA, *Global State of Scams 2025*

² Australie : Plus de 108 000 signalements d'arnaques au premier semestre 2025, avec des pertes totales s'élevant à **173,8 millions de dollars australiens**, en hausse de **26 %** par rapport à la même période en 2024 (ASC, *National Anti-Scam Centre calls for continued action this Scams Awareness Week as scam losses trend up at \$174M*, 25 août 2025).

Corée : Les pertes liées aux arnaques par hameçonnage vocal entre janvier et août 2025 ont atteint **885,6 milliards de wons sud-coréens** — dépassant les pertes totales enregistrées en 2024 (854,5 milliards de wons) (*Maeil Business Newspaper, Phone Scams Now Cost Over 1 Trillion Won Annually—Voice Phishing Has Become a National Disaster*, 21 septembre 2025) ; **273 000 comptes frauduleux** détectés, liés à des publicités financières illégales et à des sollicitations d'investissement entre août 2024 et juin 2025 (*The Korea Economic Daily, FSS, Kakao, and Google Block 270,000 Illegal Ads... Full Expansion of Co-Regulation*, 5 août 2025).

Royaume-Uni : La **Financial Conduct Authority (FCA)** a retiré ou modifié **19 000 publicités financières inappropriées ou illégales** en 2024 — soit presque le double par rapport à l'année précédente (FCA, *FCA steps up action against misleading financial adverts*, 2 juillet 2025).

nouveaux entrants sur le marché – sont parfaitement légitimes, et il est important de veiller à ce qu’ils puissent accéder à la publicité numérique avec un minimum de friction. Cependant, cette population pose également des défis de vérification que les escrocs cherchent à exploiter, en ciblant délibérément les points de l’écosystème où la surveillance est la plus difficile à appliquer de manière systématique et à grande échelle.

Le rôle de la Chambre de commerce internationale (ICC)

Par l’intermédiaire de sa **Commission mondiale du marketing et de la publicité**, l’ICC s’engage depuis longtemps à promouvoir des normes éthiques élevées en matière de marketing et de publicité, notamment par le biais du **Code ICC de la publicité et des communications marketing** (le Code ICC)³, un cadre mondial pour des communications marketing responsables. En promouvant l’**autorégulation** dans le secteur des entreprises conformément à des normes éthiques et juridiques mondialement reconnues, les consommateurs peuvent avoir confiance dans le fait que les entreprises respectant le Code ICC et les lignes directrices connexes de l’ICC fournissent une publicité **légitime, décente, honnête et véridique**, favorisant ainsi un marché robuste qui stimule la créativité tout en préservant la confiance des consommateurs.

L’approche de l’ICC en matière de prévention des arnaques reconnaît que la publicité frauduleuse exploite souvent la confiance des consommateurs par le biais de l’**usurpation d’identité** et de l’utilisation abusive d’identités de marques connues, de contenus protégés par des droits d’auteur ou d’autres actifs protégés. En pratique, les signalements basés sur la **propriété intellectuelle (PI)**, la vérification des marques et les mécanismes de notification et de retrait constituent donc une partie importante du paysage plus large de l’application des règles, aux côtés des mesures au niveau des plateformes. Bien que ce document se concentre sur les interventions spécifiques à la publicité, ces questions sont abordées dans le cadre des travaux plus larges de l’ICC sur la propriété intellectuelle, la cybersécurité et son cadre politique sur la prévention de la fraude en ligne et de la fraude facilitée par les technologies de l’information et de la communication (TIC).

Le rôle de la Global Anti Scams Alliance (GASA)

La **GASA** est une coalition mondiale à but non lucratif engagée dans la protection des consommateurs du monde entier contre les arnaques grâce à une **collaboration intersectorielles**, à la recherche et au développement de **bonnes pratiques actionnables**. En réunissant les décideurs politiques, les forces de l’ordre, les autorités de protection des consommateurs et le secteur privé, la GASA facilite le partage d’informations et de connaissances critiques pour perturber les écosystèmes d’arnaques. Grâce à son engagement à fournir des outils concrets et à favoriser un réseau mondial d’expertise, la GASA vise à promouvoir un environnement numérique plus sûr, en donnant aux parties prenantes les moyens de travailler collectivement pour préserver la confiance et la sécurité des utilisateurs dans le paysage en ligne.

³ ICC, *Code de la publicité et des communications commerciales*

L'objectif de ce guide

L'objectif principal de ce document est d'établir une **orientation stratégique claire et efficace** pour le secteur afin de relever les défis posés par la publicité payante frauduleuse. En exposant ces objectifs et en partageant les bonnes pratiques, ce document vise à offrir un aperçu des mesures prises par les acteurs responsables, des pratiques efficaces qui peuvent être mises en œuvre pour soutenir les consommateurs et empêcher les mauvais acteurs d'exploiter l'écosystème publicitaire, ainsi qu'à promouvoir leur adoption sur les plateformes concernées et à l'échelle internationale. Il cherche également à articuler la valeur de la **collaboration** entre toutes les parties intéressées, des régulateurs et des forces de l'ordre au secteur privé, en passant par les acteurs techniques pertinents et les acteurs de la société civile, afin de lutter efficacement contre ce problème.

Ce guide est destiné à **compléter**, et non à remplacer, les obligations légales et réglementaires applicables. Le cas échéant, il peut également aider à identifier les bonnes pratiques qui vont au-delà des exigences légales minimales dans les domaines où une action préventive plus forte ou plus efficace est nécessaire.

Ce document vise également à servir de **cadre de référence sectoriel** pouvant aider à renforcer la confiance, la responsabilité et la cohérence au sein de l'écosystème de la publicité et du marketing.

II. Principes clés pour lutter contre la publicité frauduleuse

Prioriser la confiance et la sécurité des utilisateurs

Internet financé par la publicité repose fondamentalement sur le maintien de **normes élevées de confiance et de sécurité des utilisateurs**, qui sont sapées par la hausse des arnaques en ligne. Pour y remédier, il est urgent d'investir en continu dans le développement et l'amélioration de **politiques, produits et processus robustes** conçus spécifiquement pour protéger les utilisateurs contre les activités frauduleuses.

La confiance ne doit pas être considérée uniquement comme un résultat de la protection des consommateurs, mais comme une **condition fondamentale** pour la légitimité et l'efficacité à long terme de l'écosystème de la publicité numérique. Un Internet sain financé par la publicité dépend de la capacité des utilisateurs, des annonceurs et des intermédiaires à s'appuyer sur des systèmes **transparents, responsables et proportionnés**. Les mesures contre la publicité frauduleuse doivent donc soutenir à la fois la sécurité des utilisateurs et la **résilience globale** du commerce numérique légitime.

Une approche multicouche et réactive en matière de sécurité des annonces

Aucune méthode unique ne permet de résoudre la complexité de la lutte contre les arnaques à l'échelle mondiale. Les méthodes doivent être **régulièrement adaptées**, notamment pour faire face aux risques découlant de l'adoption par les escrocs de l'**IA générative** et des technologies de **deepfake** [hypertrucage]. Par conséquent, des **cadres multicouches et réactifs** sont essentiels. Ceux-ci doivent intégrer une vérification à des points pertinents au cours des interactions avec un annonceur et en réponse aux informations qui deviennent disponibles pour une plateforme, et être complétés par des contrôles supplémentaires. Ils doivent inclure une **analyse régulière des schémas comportementaux des annonceurs** et de leurs historiques de transactions afin de garantir que les évaluations des niveaux de risque restent à jour et que des mesures proportionnées sont appliquées en réponse aux changements de ces niveaux.

La nécessité d'une approche basée sur le risque et proportionnée

Les mêmes systèmes publicitaires utilisés par les escrocs pour atteindre leurs victimes sont ceux utilisés par des **millions d'entreprises légitimes** dans le monde pour toucher les utilisateurs. Un équilibre doit être trouvé entre, d'une part, la nécessité pour les entreprises légitimes d'avoir un **accès facile** aux services dont elles ont besoin et, d'autre part, la mise en place de **contrôles de sécurité** qui inhibent les mauvais acteurs (où la friction liée à la vérification et aux paramètres de sécurité des comptes peut aider à atténuer les dommages qu'ils cherchent à causer).

Pour atteindre cet équilibre, les **mesures de friction et de sécurité des comptes** imposées aux annonceurs doivent être **proportionnées au risque** qu'ils représentent pour l'écosystème. Ces mesures peuvent être d'une **intensité croissante** en fonction du niveau de risque d'un annonceur, permettant une **gestion saine des risques** tout en minimisant la charge pour les entreprises légitimes opérant dans des domaines à faible risque. En outre, la nature de la

restriction peut varier, qu'il s'agisse de limitations d'exposition, de fonctionnalités ou d'options de paiement, en fonction des signaux disponibles. Avec cette approche, la **collecte excessive de données** pour des interactions à faible enjeu est évitée et les ressources peuvent être concentrées là où le risque est le plus élevé, amplifiant ainsi la valeur de cette approche basée sur le risque.

Surveillance humaine et responsabilité

Bien que les systèmes automatisés jouent un rôle essentiel dans la détection, l'évaluation et l'atténuation des risques liés aux arnaques, la **responsabilité de la gouvernance anti-arnaque** ne doit pas être déléguée à la technologie seule. Les mécanismes de prévention des arnaques doivent rester soumis à une **surveillance humaine significative**, en particulier dans les situations à haut risque impliquant l'**usurpation d'identité**, les services financiers, la **tromperie coordonnée** ou d'autres formes de préjudice grave pour les consommateurs.

Une telle surveillance permet de s'assurer que les décisions ayant des **conséquences importantes** pour les annonceurs, les utilisateurs ou l'accès au marché restent **explicables, révisables et proportionnées**. Elle permet également de préserver la confiance dans les systèmes anti-arnaque en réduisant le risque de résultats insuffisamment sensibles au contexte, aux tactiques évolutives ou aux activités commerciales légitimes.

Les participants du secteur doivent donc veiller à ce que les outils automatisés de **vérification, détection et application** soient soutenus par des **voies d'escalade claires**, des **mécanismes de révision appropriés** et des **structures de responsabilité interne**.

Il s'agit d'un domaine en **évolution rapide** : à mesure que les **modèles de langage de grande taille (LLM)** et les capacités de l'**IA agentique** mûrissent, la capacité technique à trancher des questions complexes de risque et d'exploitation commerciale augmentera. Par conséquent, la nature de la « **surveillance significative** » pourrait passer d'une intervention manuelle à des **systèmes de responsabilité gouvernés par l'IA** capables de s'adapter au volume de la publicité numérique.

Défense collective

Aucun participant, ni aucun type de participant, ne peut à lui seul empêcher les arnaques. La **collaboration entre les secteurs public et privé** est essentielle pour monter une réponse mondiale efficace contre les mauvais acteurs. En particulier, les **réseaux de partage d'informations** qui impliquent des régulateurs, les forces de l'ordre, les plateformes, les institutions financières, les fournisseurs de télécommunications, les registraires de domaines et les industries émergent comme un modèle prometteur de **coopération public-privé**. Ceux-ci devraient offrir des opportunités de partage d'informations concernant à la fois les **tendances** et les **signaux spécifiques** qui identifient les mauvais acteurs et soutiennent des approches itératives continues pour lutter contre les arnaques. Les **cadres juridiques** qui soutiennent un tel partage d'informations, offrent des voies vers les forces de l'ordre et permettent une flexibilité dans l'approche de la lutte contre les arnaques contribueront à la défense collective.

Il convient également de prendre en compte les **mécanismes de défense et d'échange d'informations établis**, tels que ceux qui existent pour la protection de la propriété intellectuelle, afin de bénéficier des travaux existants et en cours dans ces domaines.

Une **défense collective efficace** nécessite une **action coordonnée** sur l'ensemble de l'écosystème publicitaire, y compris les plateformes, les annonceurs, les agences, les organisations d'autorégulation, les parties prenantes du secteur financier, les **signalants de confiance**, les intermédiaires techniques, les autorités publiques, telles que les ministères gouvernementaux, les régulateurs, les forces de l'ordre et les organismes de protection des consommateurs. La publicité frauduleuse exploite souvent les **lacunes** entre ces acteurs ; une **coordination plus forte** est donc nécessaire non seulement pour détecter les mauvais acteurs, mais aussi pour réduire la fragmentation des réponses et accélérer l'intervention tout au long du parcours de l'arnaque.

III. Bonnes pratiques pour les plateformes, les agences et autres acteurs afin de lutter contre les arnaques

Les entités qui entretiennent des **relations directes avec les annonceurs**, en particulier les plateformes et les agences, doivent adopter et faire évoluer en continu les meilleures pratiques afin d'**atténuer les risques** et de **protéger les consommateurs**. La section ci-dessous expose les **bonnes pratiques actuelles** liées aux principes clés de la lutte efficace contre les arnaques par les plateformes publicitaires et les agences. Au cœur de celles-ci se trouve une **évaluation du niveau de risque** des annonceurs spécifiques, de leur contenu et de leur comportement, ce qui fournit une **base structurelle solide** aux efforts anti-arnaque.

A. Systèmes de vérification progressive basés sur le risque

Plateformes

⇒ Évaluations initiales

Une **protection solide contre les mauvais acteurs** peut être mise en place dès le début de la relation entre une plateforme publicitaire et les annonceurs. Un **système de vérification à plusieurs niveaux** mis en œuvre à ce stade agit comme un **contrôle de sécurité intelligent « à l'entrée »** pour l'écosystème publicitaire, empêchant les acteurs malveillants à la source, avant que des publicités préjudiciables ne puissent atteindre les consommateurs. Une approche flexible, permettant une **vérification standard** pour les annonceurs non considérés comme à haut risque, garantit que les entreprises légitimes – en particulier les **PME** – peuvent opérer sans friction excessive. Les étapes **1, 2A, 2B et 3** ci-dessous reflètent les meilleures pratiques en matière d'évaluation et de réponse aux risques posés par les nouveaux annonceurs. Elles fournissent un cadre dans lequel des **niveaux supplémentaires de contrôles** peuvent être mis en œuvre si nécessaire.

Étape 1 : Évaluations de confiance pour tous les annonceurs

Les plateformes doivent appliquer des **systèmes et processus proportionnés** pour réaliser une **évaluation initiale de la confiance** pour chaque annonceur peu après la création du compte, dans le cadre du processus d'intégration de l'annonceur (ou au moment où la conversion d'un compte utilisateur en compte annonceur payant a lieu). Cette évaluation initiale, effectuée **avant l'affichage du contenu publicitaire**, doit être basée sur des **signaux comportementaux et relationnels raisonnablement disponibles et proportionnés** pour déterminer une **classification initiale des risques** et doit inclure des mesures pour identifier les annonceurs précédemment **résiliés ou suspendus**. Les plateformes doivent maintenir leurs critères à jour pour garantir leur pertinence.

Étape 2a : Annonceurs évalués comme à haut risque lors de l'évaluation de confiance

Cette mesure s'applique aux annonceurs identifiés comme **à haut risque** à l'issue d'une évaluation de confiance.

Pour ces annonceurs, la plateforme doit :

a. exiger que l'annonceur **complète une vérification renforcée** ; b. **empêcher l'annonceur de diffuser des publicités** sur le service de la plateforme jusqu'à ce que celle-ci soit **raisonnablement convaincue**, après la réussite de la vérification renforcée, que l'annonceur ne présente pas un **risque significatif**.

La **vérification renforcée** doit impliquer un **processus de vérification à haute assurance**. Par nécessité, celui-ci évoluera avec le temps, mais il inclura probablement la vérification :

- de **l'identité de l'individu** effectuant le processus à l'aide de méthodes fournissant un **niveau élevé d'assurance** ;
- du fait que **l'annonceur est affilié à l'entreprise** au nom de laquelle il prétend faire de la publicité ;
- des **informations de base sur les opérations commerciales** de l'annonceur.

Il est probable qu'au sein de la cohorte à haut risque, il existe une marge supplémentaire pour adapter les méthodes de vérification à la **nature et à la gravité du risque**. Bien que l'**Identity Assurance Level 3** (norme **NIST 800-63A**) puisse être nécessaire dans certains scénarios à haut risque très spécifiques, il peut également représenter une **friction significative** pour de nombreuses entités commerciales légitimes. Par conséquent, le développement de **normes intermédiaires supplémentaires** pour le commerce numérique pourrait aider à soutenir cette approche équilibrée.

Étape 2b : Vérification standard des annonceurs pour tous les autres annonceurs

Pour tous les annonceurs **non classés** dans la cohorte à haut risque lors de l'étape d'évaluation de la confiance :

Pour ces annonceurs, la plateforme peut autoriser l'annonceur à **diffuser des publicités** après l'achèvement de l'évaluation initiale de la confiance et doit :

- a. exiger que l'annonceur **complète la vérification de l'annonceur** dans un **délai raisonnable** après l'intégration ;
- b. **suspendre la capacité de l'annonceur à diffuser des publicités** si celui-ci n'a pas réussi à compléter avec succès la vérification de l'annonceur.

Un tel **processus de vérification de base** requis pour tous les annonceurs non classés dans la cohorte à haut risque peut vérifier :

- **l'identité légale** de l'individu effectuant le processus ;
- **le nom légal** de l'organisation au nom de laquelle il fait de la publicité.

Ce processus peut être mis en œuvre à l'aide de **méthodes automatisées** pour faciliter l'accès à la publicité numérique et permettre de répondre à toute **exigence de transparence** pertinente. Dans ce contexte, les **identités numériques** peuvent être un outil utile pour la

standardisation et offrir une méthode **peu contraignante et hautement sécurisée** d'établissement de ce niveau d'assurance.

Étape 3 : Exigences supplémentaires pour les annonceurs de services financiers

En plus des exigences de vérification ci-dessus, pour les annonceurs de **produits ou services financiers** que les plateformes ont observés comme étant **vulnérables à l'abus** dans une juridiction pertinente, les plateformes doivent prendre des mesures pour confirmer que l'annonceur est **autorisé par le régulateur compétent** et figure sur le **registre pertinent des services financiers** (sauf si cet annonceur est **légalement autorisé** à placer des publicités payantes pour des produits ou services financiers sans autorisation supplémentaire de ce régulateur).

L'**amélioration continue des registres nationaux** est vitale pour la capacité des plateformes à mettre en œuvre ces contrôles de manière efficace. Les registres doivent être **tenus à jour, lisibles par machine** (via un accès **API ou CSV**) et **accessibles aux plateformes à grande échelle**, et doivent inclure des **champs de données** couvrant tous les **domaines** à partir desquels un fournisseur agréé est autorisé à opérer, ainsi que des **coordonnées d'entreprise actives**. **Critiquement**, les registres doivent être **mis à jour suffisamment fréquemment** pour refléter les changements de statut d'autorisation **en temps quasi réel**, garantissant que les licences **révoquées ou expirées** soient promptement reflétées et ne puissent pas être exploitées pendant l'intervalle entre la révocation et la mise à jour du registre. Il est **fortement encouragé** aux régulateurs de partager les **bonnes pratiques** en matière de normes de registre et de veiller à ce que leurs registres répondent aux **exigences minimales** énoncées à la section **IV** de ce document.

Cette mesure établit un **contrôle supplémentaire** dans un secteur à enjeux élevés où le **préjudice pour les consommateurs** peut être particulièrement grave. Une **autorisation sectorielle spécifique** confirmant que l'annonceur possède les **accréditations** pour proposer un service particulier fournit une **couche supplémentaire de friction** en plus de la vérification d'identité, qui s'applique à tous les annonceurs.

Exigences supplémentaires pour d'autres secteurs verticaux

En plus des exigences pour les services financiers ci-dessus, les plateformes doivent envisager des **exigences de vérification renforcée** pour d'autres secteurs où il existe des **preuves démontrables** de publicité frauduleuse **persistante ou systémique**, et où la vérification constitue un **moyen efficace** de déterminer le statut d'un annonceur. Les secteurs **réglementés**, y compris les **jeux d'argent** et les **produits pharmaceutiques**, méritent une **attention particulière** à cet égard. Lors de l'évaluation de la mise en œuvre de tels contrôles supplémentaires, la **qualité des données pertinentes** et la **solidité du régime réglementaire** qui y est associé sont des **considérations matérielles**.

Évaluation continue des risques et reclassification

L'**évaluation de la confiance** d'un annonceur par une plateforme doit être un **processus continu**, et non limité à un **contrôle ponctuel** lors de l'intégration, et doit utiliser une **surveillance continue** basée sur des **signaux comportementaux et relationnels raisonnablement disponibles et proportionnés**. Les plateformes doivent également s'appuyer sur des **signaux autoritaires externes**, y compris les informations partagées par les régulateurs, les forces de l'ordre, les organismes sectoriels et d'autres plateformes, **lorsqu'ils sont raisonnablement disponibles, fiables et conformes aux contraintes légales applicables**, afin de compléter leurs capacités de surveillance interne et de garantir que les évaluations des risques reflètent la **base de renseignements la plus large possible**.

Lorsque de tels signaux indiquent qu'un annonceur qui n'était **pas initialement considéré comme à haut risque** peut désormais présenter un **risque élevé** de diffusion de publicités frauduleuses, la plateforme doit exiger que cet annonceur **complète une vérification renforcée** et doit **suspendre la diffusion des publicités** jusqu'à ce que cette vérification ait été **complétée avec succès**.

Ces exigences sont **cruciales** pour lutter contre les **acteurs adverses sophistiqués** qui semblent légitimes et réussissent les contrôles initiaux avant de se livrer à des activités frauduleuses. Une **évaluation continue** garantit que la confiance n'est pas un **droit acquis à vie**, mais un **statut continu** qui doit être maintenu, permettant aux plateformes de s'adapter dynamiquement aux annonceurs dont le **profil de risque évolue** au fil du temps.

Les plateformes doivent également envisager de fournir **régulièrement des informations transparentes** à un public approprié sur l'évolution de leurs **contrôles de vérification des annonceurs et anti-arnaque**, y compris, le cas échéant, des mises à jour sur le **développement des politiques**, les **approches de vérification**, les **tendances d'abus identifiées** et les **améliorations introduites** en réponse. Une telle transparence, **à condition qu'elle ne nécessite pas de divulgation susceptible de compromettre l'efficacité des systèmes anti-fraude**, peut aider à **renforcer la responsabilité**, à **soutenir l'apprentissage du secteur** et à **encourager l'amélioration continue** au sein de l'écosystème.

Limitations proportionnées des activités publicitaires à haut risque

En plus de ce qui précède, lorsqu'un annonceur **non évalué comme à haut risque** s'engage dans des **activités publicitaires spécifiques** qu'une plateforme a observées comme étant associées à une **tendance émergente d'arnaque**, des **mesures supplémentaires** peuvent être appropriées. Ces activités peuvent inclure la tentative de diffuser des **publicités payantes** dans des **domaines thématiques à risque**. Dans ces circonstances, et en particulier si l'annonceur **ne possède pas un historique solide de publicité sûre**, la plateforme doit appliquer des **mesures proportionnées** pour atténuer les **préjudices potentiels**. De telles mesures peuvent inclure la **limitation de la visibilité** des publicités payantes de l'annonceur dans ce **domaine thématique ou cette catégorie de contenu à risque** jusqu'à ce que l'annonceur établisse un **historique suffisant de publicité sûre**.

Cette mesure permet aux plateformes d'**innover** et de développer des **outils chirurgicaux** pour gérer les **menaces émergentes** sans recourir à des **changements de politique larges et commercialement perturbateurs**. Les annonceurs doivent **gagner progressivement** le privilège d'accéder à des **domaines thématiques à risque** ou à des **fonctionnalités de produits sensibles** après avoir établi un **historique de publicité sûre**.

Agences

Les agences sont **bien placées** pour interroger l'identité de leurs clients et déterminer leur **crédibilité**. De manière similaire aux plateformes, les agences peuvent introduire une **protection solide contre les mauvais acteurs** dès le début de leur relation, et la mise en œuvre de **protocoles de connaissance du client (KYC)** permet de garantir qu'elles introduisent des **annonceurs de confiance** dans l'écosystème. Une approche flexible, permettant des **évaluations des risques** afin de déterminer où une **vigilance accrue** est nécessaire, doit être adoptée.

Les agences doivent avoir des **procédures en place** pour faciliter l'examen de **nouvelles informations** sur les annonceurs et pour effectuer le **désengagement** lorsque des annonceurs frauduleux sont identifiés.

B. Fonctionnalités complémentaires de sécurité par conception

Bien que les **systèmes de vérification** agissent comme une **porte d'entrée essentielle**, les efforts pour détecter et interrompre les escrocs ne doivent pas s'arrêter là, car les escrocs chercheront à contourner ces contrôles et peuvent **pirater des comptes légitimes** d'annonceurs (ou d'autres utilisateurs). L'**intégration et l'utilisation** de fonctionnalités de « **sécurité par conception** » par les plateformes, les agences et les annonceurs garantissent que l'écosystème publicitaire reste **résilient**, même après l'intégration d'un annonceur.

1. Mécanismes de protection robustes des comptes

La **prise de contrôle de compte** est également un **vecteur connu** pour la publicité frauduleuse. Les escrocs utilisent des **identifiants obtenus par hameçonnage** ou des **détournements de session** pour diffuser des publicités malveillantes à partir de comptes légitimes, exploitant la **confiance établie** et l'**historique de paiement** du titulaire du compte.

- **Authentification multifacteur (MFA)** : En tant que **sauvegarde** contre la prise de contrôle de compte, les plateformes doivent envisager d'exiger une **authentification multifacteur (MFA)** pour les comptes des annonceurs. Pour être efficace, les plateformes doivent promouvoir une **MFA résistante au hameçonnage** et éviter de se fier uniquement à des **formes plus faibles**, comme les **mots de passe à usage unique (OTP) basés sur les SMS**, qui sont vulnérables au **swapping de SIM**⁴ et à l'interception.
- **Intégrité des sessions et défis adaptatifs** : Les plateformes doivent mettre en œuvre des fonctionnalités qui détectent les **schémas d'accès anormaux**, tels que les **connexions depuis des lieux géographiquement éloignés** en un court laps de temps (« **voyage impossible** ») ou des **empreintes d'appareils suspectes**. Ceux-ci doivent déclencher une **réauthentification** ou un **verrouillage temporaire du compte** lorsque des **changements à haut risque** sont effectués, comme l'ajout d'une **nouvelle méthode de paiement** ou une **augmentation significative des dépenses quotidiennes**.
- **Contrôles d'accès basés sur le principe du moindre privilège** : Les agences et les grands annonceurs doivent utiliser des **paramètres de permission granulaires** basés sur le principe du **moindre privilège**. L'accès aux **fonctions sensibles**, telles que la modification des **URL de destination** ou l'exportation des listes de clients, doit être **restreint à des rôles autorisés spécifiques** afin de minimiser l'**impact potentiel** ou le « **rayon d'explosion** » d'une seule **compromission de identifiants**.
- **Application de domaines de courrier électronique d'entreprise** : Pour les comptes d'entreprise ou d'agence, les plateformes doivent offrir la possibilité de **restreindre l'accès au compte** exclusivement à des **domaines de courrier électronique d'entreprise spécifiques et vérifiés**. Cela empêche l'**accès « fantôme »** par des

⁴ transférer un numéro de téléphone sur une nouvelle carte SIM contrôlée par le fraudeur afin de recevoir les SMS, appels et souvent les codes de validation.

comptes personnels non autorisés et garantit que, lorsqu'un employé quitte une organisation, son accès peut être **révoqué centralement** via l'annuaire de l'entreprise.

2. Correction des failles courantes en matière de sécurité des annonceurs

Les escrocs exploitent fréquemment les **lacunes techniques et procédurales courantes** des entreprises légitimes. La **sensibilisation** et l'**atténuation proactive** de ces failles sont **essentiels** pour maintenir un écosystème propre.

- **Surveillance des URL de destination** : Une tactique courante consiste en le « **cloaking** », où une **URL légitime** est affichée pendant le processus de révision de l'annonce, mais est **remplacée par un site d'arnaque** une fois l'annonce en ligne. Les plateformes doivent mettre en œuvre un **balayage automatisé des pages de destination** à des **intervalles réguliers** tout au long du **cycle de vie de la campagne** pour détecter de telles **modifications non autorisées**.
- **Sécurité des API** : Pour les annonceurs et les agences utilisant des **outils automatisés**, la **sécurisation des clés API** est **critique**. Des clés compromises peuvent permettre aux escrocs de **lancer des publicités d'arnaque de manière programmatique**. Ces clés doivent être **régulièrement renouvelées** et **restreintes à des plages d'adresses IP spécifiques**.

3. Identification et prévention proactives des schémas d'arnaque récurrents

Les plateformes doivent mettre en œuvre des **systèmes proactifs** conçus pour identifier et atténuer les **schémas d'arnaque récurrents**, y compris l'utilisation d'**outils de détection de similarité** capables de signaler des **annonces substantiellement identiques** associées à des activités frauduleuses connues. Elles doivent **mettre à jour en continu** leurs méthodologies en réponse à de **nouveaux vecteurs de menace**. Une **tenue de registres efficace** et la **conservation des informations de vérification** peuvent soutenir une **détection plus efficace**.

Les plateformes doivent agir sur la base des **renseignements pertinents** provenant de **signalants de confiance** et de **partenaires du secteur** pour bloquer les **activités publicitaires frauduleuses associées** et empêcher la **réintroduction itérative** d'annonces préjudiciables.

4. Listes de blocage et enrichissement collaboratif

Les plateformes doivent **maintenir et gérer activement** des **listes de blocage** d'annonceurs frauduleux connus, de domaines, d'identifiants de paiement et d'autres signaux associés à des activités d'arnaque. Pour être efficaces, les listes de blocage doivent être traitées comme des **outils dynamiques** nécessitant des **mise à jour continues**, notamment en raison de la **facilité de création de nouveaux domaines et URL** pour héberger des contenus frauduleux et d'arnaque.

5. Éducation proactive et communication

La **communication** et l'**éducation du public** représentent une autre manière par laquelle les participants de l'écosystème peuvent contribuer à la **prévention des arnaques**. Beaucoup peuvent s'exprimer **publiquement avec autorité** sur les risques posés par les arnaques et sur la manière dont les individus et les groupes peuvent se protéger. Pour ce faire, il sera **vital** de prendre en compte les **bonnes pratiques existantes** qui favorisent l'utilisation d'un **langage informé par les traumatismes et accessible**, ainsi que l'utilisation de **campagnes d'inoculation active et d'engagement**, en plus des campagnes de sensibilisation passive. Au sein de la communauté publicitaire, il existe des **experts** qui peuvent contribuer à la **créativité** et au **savoir-faire** pour amplifier les messages et stimuler l'engagement. La participation à des **campagnes de sensibilisation** est **fortement encouragée**, bien que de telles interventions nécessitent un **suivi rigoureux** et une **évaluation**, et que les **leçons apprises** doivent être **largement partagées** au sein de l'écosystème.

Plus spécifiquement, tous les participants doivent envisager les **points de contact pertinents** avec les utilisateurs qui leur permettent de fournir des **informations et des alertes** sur les risques posés par les escrocs. Par exemple, les plateformes et les agences doivent fournir des **contrôles de santé de sécurité** ou des **tableaux de bord** qui alertent les annonceurs sur les **lacunes de sécurité**, ainsi que :

- **Notifications de point de risque** : Alertes déclenchées au moment où un utilisateur est sur le point d'effectuer une **action potentiellement risquée**.
- **Notifications de sécurité** : Alertes en **temps réel** pour les tentatives de connexion depuis de **nouveaux appareils** ou les changements apportés aux **paramètres critiques du compte**.
- **Conseils de bonnes pratiques** : Messages **clairs et actionnables** dans l'interface utilisateur concernant les risques liés à la **désactivation des fonctionnalités de sécurité** ou à l'utilisation de **méthodes d'authentification faibles**.

C. Renforcer la transparence et le contrôle utilisateur

Transparence

La **transparence des annonceurs** est un **élément fondamental** de la protection des consommateurs dans l'écosystème de la publicité numérique. Les plateformes doivent exiger des annonceurs qu'ils **divulguent leur nom officiel et leur pays d'établissement légal**, et doivent mettre ces informations à la disposition des utilisateurs **en temps réel** par le biais d'un **mécanisme de divulgation clairement accessible**, tel qu'une fonction « **À propos de cette annonce** ». Cela fournit aux utilisateurs les **moyens** de faire des **évaluations éclairées** sur la provenance des publicités qu'ils rencontrent et offre aux régulateurs et aux forces de l'ordre une **visibilité significative** sur les participants de l'écosystème publicitaire.

Les **mesures de transparence** décrites ci-dessus sont plus **facilement réalisables** lorsqu'une **relation directe** existe entre la plateforme et l'annonceur. Cependant, dans l'écosystème **programmatique ouvert**, l'**identité de l'annonceur** peut être **dissociée** de la campagne à mesure qu'elle passe par de **multiples intermédiaires** – plateformes côté demande (DSP), plateformes côté offre (SSP), bourses publicitaires et revendeurs – avant d'être publiée. Cela crée une **lacune de visibilité** dans laquelle **aucun participant unique** de la chaîne n'a une **vue d'ensemble complète** de l'identité de l'annonceur ou des **normes de vérification** qui lui sont appliquées.

Une **préoccupation particulière** est la pratique consistant à **agréger des campagnes de plateformes côté demande de niveau inférieur** et à les **revendre** à des plateformes côté demande plus premium. Cela peut effectivement permettre aux **annonceurs frauduleux** d'accéder à des **environnements d'éditeurs premium** et à des **placements publicitaires plus crédibles** sans être soumis aux **normes de vérification** que ces environnements appliqueraient aux **relations directes avec les annonceurs**. Cela crée également un **risque de réentrée** : les annonceurs **exclus d'une partie de l'écosystème** peuvent potentiellement **réintégrer** celui-ci par un **autre point de la chaîne de revente**.

Pour remédier à cela, les **plateformes, les éditeurs et les intermédiaires** opérant dans l'écosystème programmatique sont **encouragés à adopter** les **spécifications de transparence de la chaîne d'approvisionnement** de l'IAB Tech Lab, y compris **sellers.json, buyers.json, ads.txt** et l'objet **SupplyChain**. Ceux-ci fournissent l'**infrastructure de base** pour rendre les **relations de revente plus transparentes et auditable**s.

Signalement

Les **canaux de signalement** qui permettent d'**identifier les publicités suspectes ou frauduleuses** auprès des plateformes sont **vitaux** pour garantir une **défense complète** contre les arnaques et permettre la détection de **nouvelles tendances et failles**. De tels canaux de signalement doivent :

- permettre un **signalement en temps réel** avec une **identification facile** de l'actif signalé ;
- différencier le traitement en fonction du **statut du signalant**, par exemple en fournissant des **voies de signalement prioritaires** pour les **signalants de confiance**, tels que les régulateurs spécialisés, les forces de l'ordre et les organismes d'autorégulation ;
- permettre à la plateforme de **recueillir toutes les informations** dont elle a besoin pour identifier le contenu signalé, tout en restant **rapide et facile** à soumettre pour un utilisateur, et en permettant une **action rapide** de la part de la plateforme.

Les **organismes nationaux et internationaux** impliqués dans la détection des arnaques doivent se familiariser avec les **mécanismes de signalement** et collaborer avec les plateformes pour garantir une **utilisation efficace** de ces outils.

D. Participation au partage de signaux d’arnaque et de renseignements

Le **partage d’informations en temps opportun** est **central** pour lutter contre les arnaques en ligne et établir une **défense collective** contre la publicité frauduleuse. À cette fin, l’utilisation de **mécanismes d’échange de signaux en temps réel** est **fortement encouragée**. De tels systèmes doivent être guidés par des **règles clairement définies** sur la **standardisation des données**, la **vérification des informations** et les **procédures de mise à jour**, ainsi que par des **garanties de confidentialité et de sécurité**.

Étant donné la **vitesse** à laquelle les campagnes d’arnaque peuvent se propager à travers les services et les juridictions, les **mécanismes de partage de signaux rapides** sont **essentiels**. Lorsque des **indicateurs crédibles de fraude** sont identifiés, les plateformes et les **intermédiaires pertinents** doivent être en mesure d’agir **rapidement** pour examiner, suspendre ou bloquer les **publicités, comptes ou actifs connexes suspects**, tout en garantissant que de telles mesures restent **proportionnées** et soutenues par des **garanties appropriées**.

Dans la mesure du possible, les **mécanismes de partage de renseignements** doivent être conçus pour capturer **l’intégralité du parcours de l’arnaque**, et non pas seulement des **actifs publicitaires isolés**. En pratique, cela signifie permettre le signalement des **domaines liés**, des **identités des annonceurs**, des **signaux de marques clonées**, des **indicateurs liés aux paiements** et des **destinations hors plateforme**, y compris les canaux de **messagerie ou sociaux** lorsqu’ils sont pertinents. Une approche **plus intégrée** de l’échange de signaux peut **améliorer de manière significative** la détection des **récidivistes**, des **campagnes coordonnées** et de la **migration des arnaques** entre les services.

Exemple :

Global Signal Exchange⁵ (GSE), une organisation indépendante à but non lucratif basée au Royaume-Uni, qui a été cofondée par **Oxford Information Labs, Google** et la **Global Anti-Scams Alliance**, permet aux **plateformes, aux intermédiaires et aux partenaires de sécurité**, notamment les entreprises de cybersécurité et les forces de l’ordre, de **partager en temps réel des renseignements sur les menaces liées aux activités frauduleuses et aux campagnes d’escroquerie afin de faciliter la lutte intersectorielle contre ces pratiques et de promouvoir une défense collective**. Le potentiel de ces mécanismes est démontré par un **projet pilote sur la publicité malveillante** mené par l’**Advertising Association⁶** au Royaume-Uni, impliquant le GSE, Google et Amazon, qui a testé comment les **signaux de menace partagés** peuvent être mis en œuvre sur les principales plateformes afin d’identifier et de partager des **URL malveillantes**.

⁵ [Global Signal Exchange \(GSE\)](#)

⁶ [Advertising Association UK - Malvertising Pilot](#)

IV. Collaboration pour renforcer la défense collective

Une **prévention efficace des arnaques** nécessite une **coordination opérationnelle plus forte** et un **partage d'informations** entre les annonceurs, les agences, les plateformes numériques et les autres acteurs pertinents de la **chaîne de valeur publicitaire**.

La capacité de ceux qui œuvrent pour **protéger leurs services et leurs utilisateurs** contre les mauvais acteurs nécessite à la fois le **soutien des agences de régulation locales** et des **cadres législatifs** qui leur permettent de **renforcer les protections** sans augmenter leur **exposition potentielle à la responsabilité** pour les actions des mauvais acteurs.

La nature d'un tel soutien prendra des **formes différentes** au fil du temps et doit faire l'objet d'un **examen continu**. Plusieurs propositions sont exposées ci-dessous.

Cohérence et intégrité des données dans les registres nationaux

Des **registres de licences nationaux précis, accessibles et à jour** sont une **condition opérationnelle préalable cruciale** pour étendre la **vérification des annonceurs** dans les secteurs à haut risque à l'échelle mondiale. Sans des **données de registre fiables**, les plateformes ne peuvent pas **confirmer efficacement** qu'un annonceur est **légalement autorisé** à proposer les services qu'il prétend offrir, ce qui **sape le cadre de vérification** énoncé dans la **section III**.

Les **normes suivantes** sont **fortement recommandées** pour les registres de licences nationaux :

- Les **données du registre** doivent être **précises, exhaustives** et maintenues selon des **normes élevées d'intégrité des données**.
- Les registres doivent être **mis à jour suffisamment fréquemment** pour refléter les changements de **statut d'autorisation en temps quasi réel**, garantissant que les licences **révoquées ou expirées** soient **promptement reflétées** et ne puissent pas être exploitées pendant l'intervalle entre la révocation et la mise à jour du registre.
- Les données doivent être **lisibles par machine et directement accessibles aux plateformes**, par exemple via une **API ou un fichier CSV**, pour permettre des **requêtes à grande échelle** sans intervention manuelle.
- Les registres doivent inclure, **au minimum**, tous les **domaines** à partir desquels un fournisseur agréé est autorisé à opérer, ainsi que des **coordonnées d'entreprise actives**. Cela est **vital** pour atténuer le risque présenté par le **scraping de registre**, car il permet une **authentification par la plateforme**.
- Une **interopérabilité accrue** entre les registres nationaux, et le cas échéant transnationaux, **renforcerait de manière significative la vérification transfrontalière** et réduirait le risque de « **shopping de juridiction** » par les annonceurs frauduleux.

Pour les secteurs à **plus haut risque**, la **qualité, l'accessibilité et l'interopérabilité** des registres officiels ne sont pas de simples **préoccupations administratives** – ce sont des **sauvegardes opérationnelles** sur lesquelles repose une **prévention efficace des arnaques**.

Cela s'applique à tous les secteurs **licenciés et réglementés**, y compris les **services financiers**, les **jeux d'argent** et les **services de santé**, où les escrocs **usurpent fréquemment** l'identité de **firmes autorisées**, de **professionnels réglementés** ou d'**acteurs connus du marché**.

Collaboration efficace avec les forces de l'ordre et soutien aux interventions internationales

La **publicité frauduleuse** est une pratique qui **dépasse les frontières internationales**. La **perpétration** et le **préjudice** sont rarement confinés à une seule juridiction. Par conséquent, les **forces de l'ordre** et les **agences gouvernementales** doivent être **impliquées** pour **perturber les entreprises criminelles** (par exemple, les « **compounds d'arnaque** ») à leur source, et cela nécessite des **efforts internationaux** pour **partager les informations** et **encourager l'intervention**, comme détaillé dans un **briefing de l'ICC de 2026**⁷.

Promotion des « safe harbours » (zones de sécurité juridique)

Les gouvernements jouent un **rôle important** dans la création des **conditions juridiques nécessaires** à une **prévention efficace des arnaques**. Deux domaines sont particulièrement importants : les **protections contre la responsabilité** pour les actions proactives d'application, et les **cadres juridiques** qui permettent aux plateformes et autres acteurs de **partager des renseignements liés aux arnaques** sans **risque juridique excessif**.

En matière de **responsabilité**, un service ne doit pas devenir **responsable** des informations qu'il héberge simplement parce qu'il a pris des **mesures volontaires et de bonne foi** pour détecter et supprimer du contenu frauduleux. Sans une telle protection, les plateformes font face à un **incitatif pervers** à en faire **moins plutôt que plus** – les efforts proactifs d'application qui sont **imparfaits** peuvent les exposer à une **responsabilité plus grande** que de ne prendre aucune mesure. Les **protections de responsabilité « Good Samaritan »** remédient à cela en **protégeant** les plateformes et les intermédiaires contre la responsabilité découlant de leurs **efforts proactifs** pour identifier et supprimer du contenu nuisible, même lorsque ces efforts ne sont pas toujours **couronnés de succès**. La **loi européenne sur les services numériques (Digital Services Act)** et l'**article 230 du Communications Decency Act américain** sont des exemples de la manière dont de telles protections peuvent être **intégrées** dans un **cadre réglementaire plus large**.

⁷ ICC, *Preventing online and ICT-enabled fraud*, 2026

En matière de **partage d'informations**, les plateformes et les intermédiaires qui **partagent des signaux et des renseignements sur les menaces liées aux arnaques** avec d'autres participants du secteur, des régulateurs ou des forces de l'ordre doivent avoir une **certitude juridique appropriée** que le fait de le faire **de bonne foi** ne les expose pas à une responsabilité au titre des **cadres juridiques** en matière de **protection des données**, de **concurrence** ou d'autres domaines. L'**absence d'une telle certitude** est un **obstacle matériel** au type de **défense collective** que ce document prône. Les gouvernements doivent examiner si les **cadres juridiques existants** soutiennent **suffisamment** le partage d'informations de bonne foi à des fins de prévention des arnaques, et introduire des **dispositions de « safe harbour » ciblées** là où ils ne le font pas.

À propos de l'International Chamber of Commerce (ICC)

La **Chambre de commerce internationale (ICC)** est le **représentant institutionnel** de plus de **45 millions d'entreprises** dans plus de **170 pays**. La mission principale de l'ICC est de **faire en sorte que les affaires fonctionnent pour tous, chaque jour et partout**. Grâce à un **mélange unique** de plaidoyer, de solutions et d'établissement de normes, nous promouvons le **commerce international**, la **conduite responsable des affaires** et une **approche mondiale de la réglementation**, en plus de fournir des **services de résolution des litiges de premier plan**. Nos membres incluent de nombreuses **principales entreprises mondiales**, des **PME**, des **associations professionnelles** et des **chambres de commerce locales**.

À propos de la Global Anti Scams Alliance (GASA)

La **Global Anti-Scam Alliance (GASA)** est une **organisation internationale** qui réunit les acteurs des **secteurs public et privé** pour mieux **comprendre, prévenir et répondre** aux arnaques. Avec plus de **100 organisations membres** dans le monde, y compris des **institutions financières de premier plan**, des **entreprises technologiques** et des **organismes gouvernementaux**, la GASA sert de **plateforme collaborative** pour une **action coordonnée** contre les arnaques.

Les arnaques sont devenues un **problème mondial généralisé**, affectant les **individus, les entreprises et les économies** à travers les frontières. La GASA existe pour **soutenir les efforts coordonnés et intersectoriels** qui réduisent le **préjudice pour les consommateurs** et **renforcent les réponses collectives** aux activités d'arnaque.