

ÉTUDE DE CAS



## LexisNexis® Risk Solutions aide une plate-forme de voyages en ligne à réduire les usurpations de comptes et l'acquisition frauduleuse de bons d'achat

Les renseignements dynamiques sur l'identité numérique permettent de distinguer en temps réel les utilisateurs de confiance des cybercriminels

### EN BREF

#### SOCIÉTÉ

Plate-forme de voyages en ligne

#### CAHIER DES CHARGES

- Maintenir une plate-forme sécurisée, sûre et fiable pour les hôtes et les voyageurs.
- Offrir un accès fluide aux services de paiement et de réservation en ligne.
- Détecter et bloquer efficacement les usurpations de comptes.
- Empêcher les cybercriminels de monnayer les bons d'achat.

#### SOLUTION

En utilisant les renseignements dynamiques sur l'identité numérique LexisNexis Risk Solutions lors des opérations de paiement et de connexion, cette plate-forme de voyages en ligne identifie les comportements à haut risque en temps réel, ce qui lui permet de protéger l'intégrité de sa communauté.

#### CE QU'IL FAUT RETENIR

- Réduction du nombre d'usurpations de comptes.
- Diminution significative des opérations frauduleuses sur les bons d'achat.

### Présentation

Le succès de cette plate-forme de voyages en ligne repose sur la confiance réciproque entre les hôtes souhaitant louer leur bien et les visiteurs recherchant une expérience de voyage plus authentique. La protection et la sécurité sont prioritaires à tous les stades de l'aventure, que ce soit en ligne ou hors ligne, afin d'empêcher les fraudeurs d'infiltrer la communauté en ligne.

LexisNexis® Risk Solutions permet d'identifier et de bloquer les fraudeurs qui tentent de :

- Publier de faux renseignements, compromettre des comptes ou modifier les informations de compte des utilisateurs de confiance.
- Se procurer des bons d'achat numériques au moyen de cartes bancaires volées.
- Duper les visiteurs en les poussant à transférer l'argent directement sur le compte en banque d'un fraudeur au lieu d'utiliser la plate-forme de paiement.

### Enjeu commercial

Les plates-formes en ligne se sont multipliées, tout comme les cybercriminels qui cherchent à gagner de l'argent en escroquant des clients peu méfiants au moyen d'identifiants volés ou d'attaques d'ingénierie sociale. Comme cela est le cas pour l'ensemble des plates-formes en ligne et des sites de commerce électronique, les fraudeurs ciblent cette plate-forme de voyages en ligne afin d'usurper des comptes de valeur, ou de réaliser des profits via différentes escroqueries ou fraudes aux paiements.



En modifiant les informations de contact et en poussant des clients crédules à effectuer des virements en dehors de la plate-forme de paiement sécurisée, les fraudeurs peuvent réaliser des profits substantiels.

À l'instar de nombreuses entreprises en ligne, cette plate-forme souhaitait pouvoir offrir des bons d'achat numériques en toute sécurité. Cependant, cette offre était devenue une source d'activités frauduleuses. Les fraudeurs utilisaient des cartes bancaires volées pour se procurer des bons d'achat, et essayaient ensuite de gagner de l'argent en les revendant sur d'autres plates-formes en ligne ou par le biais de pratiques de réservation collusoires. Dans les deux cas, cela donnait lieu à de nombreuses vérifications manuelles et constituait un risque financier inutile.

La société avait besoin d'une solution de protection contre la fraude lui permettant de détecter les comportements à haut risque ou anormaux au moment de la connexion, et offrant une meilleure visibilité sur la signature numérique d'un utilisateur pour détecter efficacement les opérations de paiement frauduleuses.

### **Exploitation de la puissance des renseignements partagés à l'échelle mondiale pour une détection en temps réel des événements à haut risque**

La meilleure façon de lutter contre le problème complexe du cybercrime organisé est d'exploiter la puissance d'un réseau mondial partagé. Le réseau d'identités numériques Digital Identity Network® de LexisNexis® collecte et traite les renseignements partagés à l'échelle mondiale provenant de millions d'interactions client quotidiennes, dont les connexions, les paiements et les demandes de nouveau compte. Grâce à ces informations, LexisNexis® Risk Solutions crée une identité numérique unique pour chaque utilisateur en analysant les innombrables liens entre les appareils, les lieux et les informations personnelles anonymisées.

Les comportements s'écartant de cette identité numérique de confiance sont détectés avec précision et en temps réel, alertant les entreprises d'une possible tentative de fraude. Les comportements suspects sont identifiés et signalés pour vérification, authentification renforcée ou rejet avant le traitement de la transaction, ce qui réduit les contretemps pour la grande majorité des utilisateurs de confiance dans la communauté de la plate-forme de voyages en ligne.

La meilleure façon de lutter contre le problème complexe du cybercrime organisé est d'exploiter la puissance d'un réseau mondial partagé.

### Utilisation de Smart ID pour détecter les appareils suspects

Smart ID identifie les utilisateurs récurrents qui effacent les cookies, se servent de la navigation privée et modifient d'autres paramètres pour contourner la prise d'empreintes numériques des appareils. Cela améliore la détection des utilisateurs récurrents et réduit les faux positifs. À partir de l'analyse des caractéristiques d'un grand nombre de navigateurs, plug-ins et connexions TCP/IP, Smart ID détecte les tentatives de connexion multiples, par exemple de fraudeurs tentant d'usurper des comptes existants.

### Mise en lumière des comportements frauduleux en ligne

Les technologies d'analyse approfondie des connexions offrent un aperçu plus précis des événements suspects. Les fraudeurs tentent souvent de se cacher derrière des services de dissimulation de l'identité et de l'emplacement géographique, tels que des proxies cachés, des VPN et le navigateur TOR. Grâce à la technologie de perçage de proxy, LexisNexis® Risk Solutions examine les informations d'en-tête des paquets TCP/IP pour dévoiler à la fois les adresses IP de proxy et les véritables adresses IP.

Le réseau d'identités numériques Digital Identity Network® de LexisNexis® collecte et traite les renseignements partagés à l'échelle mondiale provenant de millions d'interactions client quotidiennes, dont les connexions, les paiements et les demandes de nouveau compte. Grâce à ces informations, LexisNexis® Risk Solutions crée une identité numérique unique pour chaque utilisateur en analysant les innombrables liens entre les appareils, les lieux et les informations personnelles anonymisées.



Pour plus d'informations, appelez le 866.528.0780  
ou rendez-vous sur [risk.lexisnexis.com/FIM-EN](http://risk.lexisnexis.com/FIM-EN)

#### À propos de LexisNexis Risk Solutions

LexisNexis Risk Solutions exploite tout le potentiel des données et de l'analyse avancée pour fournir des informations qui aident les entreprises et les pouvoirs publics à réduire les risques et à prendre des décisions plus éclairées visant à rendre le monde plus sûr. Nous proposons des solutions technologiques et des données dans de nombreux secteurs d'activité, notamment les assurances, les services financiers, la santé et le service public. Basée à Atlanta, Géorgie, la société est implantée dans le monde entier et fait partie de RELX Group (LSE : REL/NYSE : RELX), fournisseur mondial de solutions d'information et d'outils d'analyse pour les professionnels dans tous les secteurs d'activité. Membre du FTSE 100, RELX est basé à Londres. Pour plus d'informations, rendez-vous sur [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com) et [www.relx.com](http://www.relx.com)

#### À propos de ThreatMetrix

ThreatMetrix®, société de LexisNexis® Risk Solutions, permet à l'économie mondiale de connaître une croissance rentable et sûre, sans compromis. Grâce à une vision complète sur 1,4 milliard d'identités numériques tokenisées, LexID® Digital fournit des renseignements sur lesquels s'appuient 110 millions de décisions quotidiennes d'authentification et de confiance afin de distinguer en temps réel les clients légitimes des fraudeurs. Dans l'étude Forrester Wave™ de 2017, ThreatMetrix est reconnu comme l'unique leader du marché de l'authentification basée sur les risques.

Pour en savoir plus, rendez-vous sur [www.threatmetrix.com](http://www.threatmetrix.com).

LexisNexis, LexID et le logo Knowledge Burst sont des marques déposées de RELX. ThreatMetrix et Digital Identity Network sont des marques déposées de ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions. NXR14085-00-0919-EN-US