LIVRE BLANC | OCTOBRE 2014

Authentification 3D Secure basée sur des modèles avancés

Les modèles d'authentification basée sur le comportement et les risques utilisés dans le cadre des transactions de commerce en ligne permettent de réduire les pertes et d'assurer le bon déroulement des transactions à faible risque.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, Advanced Analytics and Data Science

ca technologies

Table des matières

Résumé

Défi

Les organismes émetteurs de cartes bancaires sont tenus de trouver le juste équilibre entre la sécurité des transactions de commerce électronique et une expérience de paiement agréable pour les clients. Le nœud du problème consiste à trouver le moyen de fournir une expérience de règlement des transactions conviviale pour les clients légitimes (afin qu'ils ne renoncent pas à leurs transactions ou n'optent pas pour une autre forme de paiement), tout en prévenant les tentatives de fraude. L'utilisation d'une authentification basée sur le comportement, visant à identifier les transactions dans le cadre desquelles le client doit fournir des moyens supplémentaires d'authentification, est un point essentiel : en effet, elle va permettre de réduire le phénomène de frustration pour le client tout en renforçant la fiabilité de ses transactions. Si les règles constituent un composant important de cette authentification, l'ajout et l'utilisation de modèles visant à guider l'application de ces règles permettent de renforcer considérablement leur efficacité pour prévenir les tentatives d'authentification illégitimes, tout en réduisant leur impact sur les clients légitimes. Les titulaires de carte bénéficient ainsi d'une meilleure expérience, tandis que les organismes émetteurs limitent leurs pertes financières liées aux fraudes.

Solution

Le canal 3D Secure présente de nombreuses opportunités pour les organismes émetteurs de cartes. Au vu de l'augmentation importante des fraudes dans le secteur du commerce électronique et dans le contexte du transfert de responsabilité (« liability shift »), l'authentification 3D Secure offre une première ligne de défense aux organismes émetteurs. Il importe cependant de faire bon usage de cette première ligne de défense et de l'utiliser à bon escient. CA Risk Analytics permet d'examiner la transaction de commerce en ligne au moment de l'authentification de l'acheteur à l'aide d'informations uniques auxquels les systèmes de détection des fraudes actifs n'ont pas accès au moment de l'autorisation, ce qui lui permet de prévenir les transactions illégitimes. Une évaluation du risque d'authentification doit être effectuée afin d'offrir une expérience d'achat ininterrompue à la majorité des titulaires de cartes légitimes. En déployant CA Risk Analytics, les organismes émetteurs peuvent ainsi réduire leurs pertes et limiter la frustration du client.

Avantages

CA Risk Analytics peut aider les organismes émetteurs à évaluer le niveau de risque des activités en ligne sur les sites des commerçants 3D Secure. Le système évalue en temps réel et en toute transparence le risque qu'une transaction de commerce en ligne ait été initiée par une personne autre que le titulaire légitime de la carte de paiement. Il peut ainsi identifier une part importante des tentatives de transaction légitimes et autoriser directement les clients concernés à poursuivre leurs achats sans impact, tout en détectant de la même manière les tentatives de transaction illégitimes qui doivent être bloquées. L'identification de l'appareil, les données de géolocalisation, les caractéristiques de la connexion ainsi que les schémas historiques sont autant d'informations qui peuvent être utilisées pour l'évaluation du risque de chaque tentative de transaction.

CA Risk Analytics se distingue notamment par le fait qu'il dispose de modèles régionaux avancés utilisant des capacités d'analyse sophistiquées, notamment un modèle de réseau neuronal et comportemental, pour fournir une évaluation du niveau de risque de chaque tentative. Les règles intégrées dans CA Risk Analytics peuvent ensuite combiner ce score avec d'autres facteurs métier afin de déterminer la suite à donner à chaque tentative de transaction. L'ensemble de la solution gagne ainsi considérablement en efficacité.

Section 1

3D Secure fournit la base pour réduire les pertes dans le cadre du commerce en ligne

Le protocole 3D Secure offre aux organismes émetteurs de nombreuses opportunités de tirer pleinement parti des avantages et de la protection offerte par le canal 3D Secure.

Le rôle du canal 3D Secure est d'authentifier les tentatives de transactions de commerce électronique. Avant d'aller plus loin, il convient de bien comprendre la différence entre authentification et autorisation : l'authentification est le processus visant à tenter de confirmer que la personne à l'origine d'une transaction (ou d'une autre activité) au moyen d'une carte de paiement est bien le détenteur légitime et réel de cette carte. L'autorisation est le processus visant à tenter de valider que le détenteur de la carte de paiement (confirmé) est autorisé à réaliser la transaction (sur la base des politiques en place, du solde de la carte, de l'état de son compte et d'autres facteurs). Une fraude peut survenir et être détectée aussi bien dans la phase d'autorisation que dans la phase d'authentification, avec des différences notables : ainsi et par exemple, le processus d'authentification ne permet pas de prévenir directement les fraudes de première partie. Cependant, quel que soit le type de fraude, le fait d'authentifier la personne tentant d'effectuer une transaction constitue le point de départ de la procédure qui permettra de garantir la validité de la transaction proprement dite.

Dans le cadre de transactions avec carte, la présence physique de la carte est acceptée depuis longtemps à titre d'élément clé de l'authentification. Pour répondre aux attaques de plus en plus sophistiquées des utilisateurs illégitimes, les organismes émetteurs ont renforcé la sécurité des cartes (bande magnétique, numéros CVV/CVC/CID et cartes à puce). Ces informations d'authentification sont généralement transmises à la demande d'autorisation.

Dans le cadre de transactions sans carte (Card Not Present, CNP), l'authentification physique au moyen de la carte n'est plus possible et c'est généralement le commerçant qui assume la responsabilité de l'authentification. Toutefois, l'avènement du commerce en ligne a nécessité la mise au point d'une authentification robuste des transactions de commerce électronique. En effet, si les données fournies au moment de la demande d'autorisation sont suffisantes pour autoriser une transaction, elles ne suffisent cependant pas pour authentifier une transaction de commerce en ligne. C'est la raison pour laquelle la transaction 3D Secure a été créée : une transaction 3D Secure requiert des informations différentes de celles fournies dans la demande d'autorisation, afin d'authentifier la personne à l'origine de la transaction. Cette tâche fondamentalement différente du processus d'autorisation, nécessite une perspective unique. En revanche, les résultats de cette authentification peuvent être exploités dans le flux d'autorisation afin de fournir un meilleur contexte au système d'autorisation.

Pour plus de clarté, l'utilisation du mot « fraude » dans ce document fera référence à une fraude d'authentification dans le cadre de transactions 3D Secure de commerce en ligne.

Le protocole 3D Secure permet d'examiner les tentatives d'authentification en utilisant des informations uniques qui ne sont pas disponibles pour les systèmes de détection des fraudes et d'autorisation, pour prévenir ainsi les transactions illégitimes avant même qu'elles ne déclenchent des demandes d'autorisation. Les informations uniques utilisées par le système CA Risk Analytics comprennent un ID unique associé à chaque terminal (ID du périphérique), l'URL à laquelle le titulaire de la carte accède pour exécuter la transaction (URL du commerçant), l'adresse IP actuelle de son terminal, ainsi que des informations annexes de fournisseurs de données tiers, notamment l'emplacement du terminal, la vitesse et le type de connexion, l'identification des anonymiseurs et d'autres informations. Ces informations s'ajoutent (sans les remplacer) aux informations habituelles déjà disponibles (montant, devise de la transaction, nom et ID du commerçant, identifiant de la carte, etc.). Les modèles d'authentification 3D Secure offrent ainsi plus d'avantages que les modèles d'autorisation qui ne prennent en compte que les informations habituelles, et offrent une détection forte des tentatives d'authentification illégitimes tout en ayant un impact limité sur les tentatives de transaction légitimes.

Le canal 3D Secure fournit des informations en temps réel pour permettre l'analyse des transactions d'authentification : il permet en particulier de mettre à jour les informations concernant la carte, le terminal ou d'autres entités pivots intervenant dans la transaction en temps réel. Dans ce système, les transactions suivantes bénéficieront de ces informations et de ce contexte enrichis au moment où le système évaluera leur risque d'authentification. Le résultat peut être particulièrement puissant dans le cadre de l'analyse d'entités opérant entre des institutions dans un environnement SaaS Cloud.

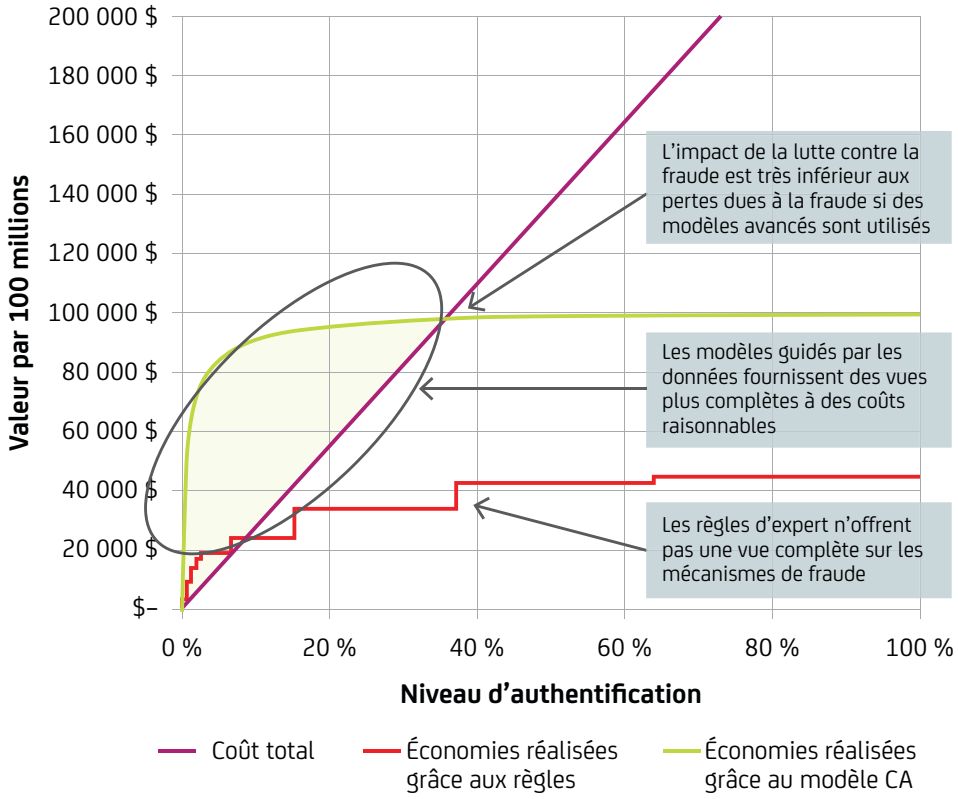
À cela s'ajoute la capacité d'éliminer le phénomène de frustration de l'expérience d'achat en ligne. Les premiers déploiements 3D Secure posaient des questions de sécurité aux clients des sites marchands. Si leur niveau de sécurité est fort, par exemple l'utilisation de systèmes de mots de passe à usage unique (one-time-passwords, OTP), ces déploiements peuvent être relativement efficaces ; mais lorsque ce niveau est faible, notamment la demande d'informations pour pouvoir exécuter la transaction proprement dite (date d'expiration ou code CVV2), alors le déploiement 3D Secure ne permettra pas vraiment de réduire les pertes financières liées aux fraudes. Il convient en outre de prendre en compte la frustration introduite par les questions de sécurité, laquelle a pour effet d'augmenter la réticence du client à finaliser la transaction et exerce un impact négatif sur l'expérience du client.

L'impact négatif de la frustration dans le cadre de l'expérience client n'est pas seulement qualitatif, mais quantitatif, car il contribue à accroître considérablement les taux d'abandon et de « faux échec », avec pour conséquences principales une baisse des commissions d'interchange, mais aussi des soldes disponibles sur les cartes de crédit, voire une érosion du nombre de clients (un problème important tant pour les comptes de débit que de crédit). Quantifiables, ces pertes motivent fortement les organismes émetteurs à tenter de réduire la frustration engendrée par les transactions et ainsi améliorer l'expérience de leurs clients. Si tous les clients devaient systématiquement répondre à des questions de sécurité au moment d'effectuer leurs achats en ligne, les coûts liés aux abandons de transactions pourraient dépasser le montant des éventuelles pertes. Par conséquent, il convient d'évaluer le risque d'une transaction donnée, afin d'intervenir uniquement lorsque cela est clairement justifié. L'authentification basée sur le comportement est le meilleur moyen de réaliser cette évaluation.

L'illustration 1, sur la page suivante, montre un exemple de coût total des systèmes de détection des fraudes (incluant les opportunités perdues du fait de l'abandon des transactions, ligne violette), les économies réalisées au moyen d'un système standard fonctionnant sur la base de règles (ligne rouge), et celles que permet de réaliser un modèle régional utilisant CA Risk Analytics (ligne verte). Notez que plus le niveau de sécurisation augmente, plus le coût d'exploitation du système augmente lui aussi. Avec un système basé sur des règles, qui ne permet généralement pas de disposer d'une vue complète sur le phénomène de fraude, le coût d'exploitation du système peut rapidement dépasser le montant des économies qu'il permet de réaliser. Avec un modèle avancé basé sur des données, il est possible d'obtenir une vue d'ensemble sur la fraude moyennant un coût raisonnable. La zone en vert illustre l'avantage du modèle sur les règles.

Illustration 1.

Coût total de la détection des fraudes.



Section 2

Authentification fondée sur le comportement

L'authentification basée sur le comportement implique de placer la transaction en contexte en la comparant aux schémas d'utilisation habituels du titulaire de la carte, du commerçant et du terminal utilisé. Il est ainsi possible de vérifier si ces informations seules permettent d'avoir la quasi certitude que la personne à l'origine de la transaction est bien le titulaire de la carte. Dans l'affirmative, inutile d'ennuyer le payeur pendant sa transaction : celle-ci peut être exécutée sans procédure supplémentaire, ce qui permet de réduire de manière significative la frustration et la probabilité de renoncement, mais aussi d'améliorer l'expérience du titulaire de la carte[1]. En revanche, si la transaction est suspectée de ne pas être effectuée par le titulaire de la carte, elle peut être refusée immédiatement, empêchant ainsi toute demande d'autorisation ou de règlement, ce qui permet d'éviter les risques de fraude, y compris dans le cas où le fraudeur connaîtrait les informations d'authentification. Pour finir, dans le cas des transactions pour lesquelles le niveau de légitimité ne peut pas être déterminé, il est recommandé d'avoir recours à une interaction d'authentification forte avec le titulaire de la carte. L'idée maîtresse de l'authentification basée sur le comportement est d'exploiter des schémas comportementaux afin de réduire l'incertitude concernant la légitimité de la personne qui tente de s'authentifier en tant que titulaire de la carte, et ainsi (a) de limiter le pourcentage de transactions légitimes soumises à une authentification secondaire (b) tout en garantissant qu'un plus grand nombre de cas de fraude se voient confronter à cette authentification secondaire, (c) et soient donc directement refusés.

Modèles en tant qu'instruments d'authentification basés le comportement

Les modèles régionaux CA Risk Analytics sont conçus sur la base de données des organismes émetteurs régionaux, qui autorisent l'utilisation de leurs données dans le CA eCommerce Consortium et contribuent ainsi au processus « truth data »[2]. Les données concernées comprennent des transactions 3D Secure de cartes de crédit et de débit.

Les modèles régionaux englobent un certain nombre d'éléments différents, et en premier lieu les informations de la transaction en cours : la date et l'heure, le montant, l'emplacement de la personne qui tente de s'authentifier pour la transaction (c'est-à-dire l'ordinateur ou le terminal mobile du titulaire de la carte dans le cas d'une transaction de commerce en ligne), le nom, l'ID et l'URL du commerçant, les informations sur l'adresse IP du terminal, les caractéristiques de la connexion, ainsi que les informations auxiliaires provenant de fournisseurs de données tiers. Si ces données sont essentielles, dans la mesure où elles permettent au modèle de comprendre la transaction en cours, elles ne permettent pas de comprendre les comportements impliqués.

Dans un deuxième temps, les modèles exploitent les informations issues des comportements précédents pour les entités pivots de la tentative d'authentification actuelle (carte, terminal ou commerçant par exemple). Les informations des comportements passés sont extraites dans les facteurs importants afin d'identifier les schémas comportementaux. Il peut s'agir des sites de commerce électronique visités par le client, des montants de ses achats, des emplacements et des terminaux utilisés pour chacune de ces visites, ainsi que les terminaux uniques utilisés avec la carte de paiement. Des schémas similaires sont également observés sur d'autres entités pivots. Ces condensés ou historiques, sont mis à jour à chaque tentative d'authentification d'une transaction.

En troisième lieu, les modèles utilisent des variables complexes, incluant des mini-modèles, qui isolent les schémas comportementaux des pivots impliqués dans la transaction, et déterminent comment et si la transaction en cours suit ces schémas. Ces variables peuvent par exemple détecter l'utilisation d'un nouveau terminal pour une carte donnée ou le rythme des dépenses enregistrées sur une carte ou un terminal. Plus complexes, elles peuvent servir à comparer la tendance d'un titulaire de carte à opérer des achats récurrents ou encore le nombre de ses visites sur un site marchand par rapport à d'autres personnes.

Quatrièmement, les modèles utilisent des tables conçues sur la base de données historiques : ces tables fournissent des informations sur les tendances passées en matière de transactions légitimes et frauduleuses dans les données historiques et incluent des tendances et classificateurs bayésiens naïfs.

Enfin, tous ces éléments sont présentés à un modèle numérique non linéaire qui pondère leurs prédictions concernant des anomalies comportementales et le risque de tentative illégitime. Ces modèles capturent les comportements non linéaires : les relations importantes entre variables et la probabilité de fraude qui ne sont pas une simple relation linéaire. Ils comparent les indicateurs de risques (par ex. : il s'agit d'un commerçant présentant un taux de fraude élevé) avec des facteurs de pondération (par ex. : cette personne a déjà exécuté ce type de transaction sur ce terminal) en observant de nombreuses relations.

La façon dont les différents facteurs sont pondérés est déterminée à l'aide d'un algorithme d'apprentissage sur un grand ensemble de données de transactions historiques et les « truth data », autrement dit, ces types de modèles sont « guidés par des données ». Ces modèles peuvent donc détecter des relations non triviales qui ne sont pas aisées à capturer dans des règles, pour présenter la meilleure évaluation de la probabilité qu'il s'agisse de transactions illégitimes.

Ils génèrent un score numérique qui correspond à une estimation de la probabilité que la tentative d'authentification soit *illégitime*. Ce mécanisme permet un classement des transactions d'authentification, et l'exécution de différentes actions classées en fonction de leur priorité. En particulier, il autorise la mise en place d'une « authentification silencieuse » des transactions qui n'affecte pas le détenteur de la carte lorsque le schéma comportemental indique une faible probabilité de fraude.

Modélisation numérique non linéaire exploitant des réseaux neuronaux sans rétroaction

Si les approches numériques disponibles sont nombreuses, les réseaux neuronaux sans rétroaction (feed-forward neural networks, FFNN) offrent la combinaison idéale entre performances, flexibilité et faisabilité.

Ces réseaux sont extrêmement flexibles, car ils ne nécessitent aucune assomption structurelle ou de distribution dans l'espace des entrées/fonctionnalités. Ils affichent des performances de pointe même avec des données les moins linéaires, car ce sont des instruments universels d'approximation de fonctions. De plus, indépendamment de la taille ou de la complexité des données, ils apprennent en temps linéaire et génèrent un score en temps constant, ce qui les rend efficaces dans l'analyse d'ensembles de données très volumineux.

Structure des réseaux neuronaux

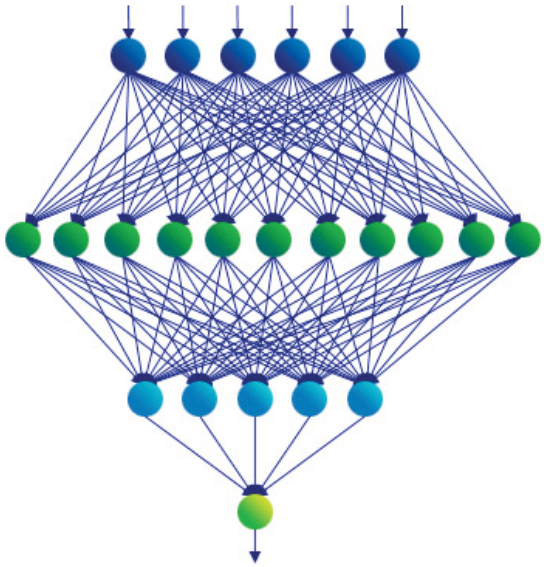
Un réseau FFNN est, en substance, un graphique de flux de signaux acyclique orienté non linéaire, dont l'entrée est une représentation numérique de la transaction telle qu'elle a été capturée par les techniques décrites précédemment ; le résultat, dans ce contexte, est une mesure ordinale de la probabilité que la tentative d'authentification soit frauduleuse (score).

En clair, un réseau FFNN peut être décrit comme une séquence de « couches », chacune se composant d'un ensemble de « neurones » (voir illustration 2). La tentative d'authentification de l'entrée est présentée à la première couche (entrée), avant de se propager à travers le réseau. La propagation se poursuit à travers les couches internes (« couches masquées »), jusqu'à la couche de sortie. Chaque couche opère une transformation non linéaire sur l'entrée et transmet les résultats à la couche suivante. Chaque couche peut avoir un nombre arbitraire de neurones : dans le contexte actuel, la couche finale (sortie) n'utilise qu'un seul neurone (pour produire le score).

L'expressivité des réseaux FFNN réside dans ces transformations séquentielles non linéaires qui, collectivement, permettent au réseau de modéliser chaque fonction d'une entrée.

Illustration 2.

Exemple de réseau neuronal sans rétroaction (FFNN).



Section 3

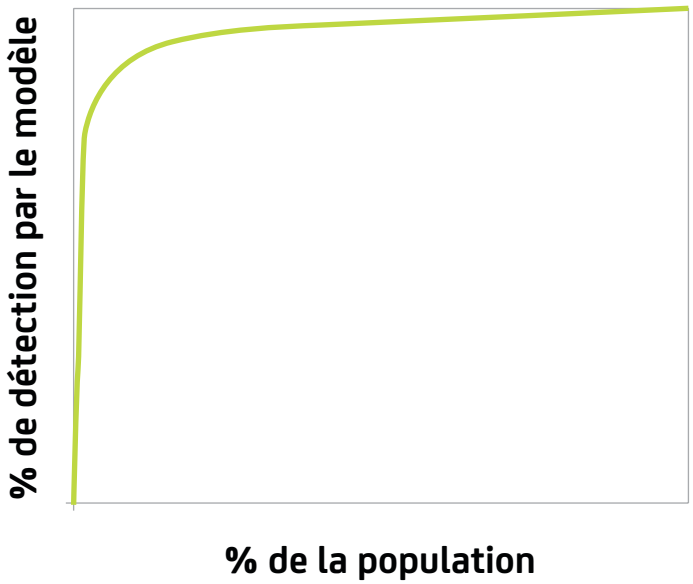
Avantage des modèles avancés

Performances des modèles

Les modèles CA régionaux permettent le rejet ou le renforcement de l'authentification d'une majorité des transactions frauduleuses tout en n'affectant qu'un nombre restreint de transactions légitimes. Les performances générales sont montrées dans l'illustration 3. Le modèle optimise la détection des fraudes tout en minimisant l'impact sur les clients. Notez que la courbe complète n'est pas visible ici : seule sa zone opérationnelle est représentée.

Illustration 3.

Détection des fraudes du modèle en tant que fonction du pourcentage de toutes les transactions détectées par le modèle. Notez que le graphique couvre seulement une portion de la population, se concentrant sur la zone opérationnelle de la courbe.



Scores et règles des modèles

Les règles sont des outils très performants pour cibler des indicateurs précis et connus de fraude. Elles sont en outre rapides à mettre en œuvre et facile à comprendre. Cependant, comme elles ne sont pas guidées par les données, leur efficacité se limite à l'étendue des connaissances de leur rédacteur dans le domaine des signaux de fraude. Les règles ne permettent pas de capturer des comportements complexes facilement, ni de combiner des risques multiples dans une décision spécifique. Elles ne peuvent pas non plus classer les transactions en vue de déclencher leur rejet, une phase d'authentification secondaire ou encore un ajustement de leur volume.

De leur côté, les modèles capturent des schémas complexes en exploitant des variables sophistiquées. Ces variables sont basées sur la transaction en cours ainsi que sur les condensés pivots (informations clés de transactions passées sur les identifiants pivots de transactions). Grâce à l'utilisation combinée de variables non linéaires et linéaires, ainsi que des techniques d'apprentissage établies, les modèles peuvent pondérer les différents facteurs sur la base d'une approche guidée par les données, et ainsi produire un classement des transactions par niveau de risque de fraude. Comme les modèles ne permettent pas d'initier des actions, les règles sont leur complément essentiel.

Combinaison de règles et de modèles

Vu leurs différents points forts, la meilleure approche consiste à associer modèles et règles. Dans un premier temps, un modèle fort distingue les cas de fraude possibles, puis classe les transactions concernées en leur attribuant des scores. Ensuite, il s'agit d'écrire des règles qui utilisent ce score de différentes manières : (i) les scores élevés, qui indiquent une forte probabilité de fraude, doivent servir à déclencher des actions (le score servant de seuil de déclenchement sera défini en fonction du volume et du niveau de fraude déterminés par l'institution cliente) ; (ii) les scores les plus faibles peuvent être combinés avec des règles dont le rôle est de filtrer les transactions présentant une forte probabilité de légitimité, ce qui permet aux autres règles de traiter un ensemble de données plus riche. Enfin, l'organisme pourra mettre en œuvre des règles de stratégie indépendantes du niveau de risque de fraude, qui dicteront par exemple le déclenchement d'une authentification secondaire pour les nouveaux terminaux.

Section 4

Conclusion

L'utilisation d'une authentification basée sur le comportement afin de déterminer quelles transactions doivent être soumises à une authentification secondaire ou directement refusées est indispensable pour réduire l'impact sur le client, tout en offrant de meilleures garanties concernant la légitimité des transactions. Si les règles constituent un composant important de cette authentification, elles connaissent un certain nombre de limites. À condition d'associer aux règles des modèles basés sur une analyse du comportement et de guider leur application, il est possible de renforcer de manière significative leur efficacité sur les tentatives d'authentification illégitimes, tout en réduisant leur impact sur les clients. Ces derniers bénéficieront ainsi d'une meilleure expérience, tandis que les organismes émetteurs pourront réduire leurs pertes financières liées aux fraudes.

Section 5

À propos des auteurs

Paul Dulany travaille dans le secteur de la science des données et de l'analyse avancée depuis 14 ans. Après avoir rejoint CA Technologies en 2013, il a supervisé le développement de l'infrastructure de modélisation analytique et du premier modèle produit par l'équipe CA Data Science. Avant de rejoindre CA Technologies, il a travaillé auprès de SAS Institute pendant huit ans et faisait partie de l'équipe qui a conçu les premières versions de la solution SAS Enterprise Fraud Management. Il a également supervisé le développement des premiers modèles de cartes de débit et de nombreuses autres techniques. Avant cela, il a travaillé auprès de HNC et de Fair Isaac pendant plus de cinq ans, en tant que scientifique, puis en tant que responsable de l'équipe Fraud Predictor Modeling, développant notamment un certain nombre de modèles de cartes de paiement Falcon. Paul détient plusieurs brevets issus de son travail auprès de HNC et SAS, et est titulaire d'un doctorat en physique théorique.

Hongrui Gong dispose d'une grande expérience dans le domaine de la science des données et de l'analyse avancée. Recruté par CA Technologies en avril 2013, il a joué un rôle clé dans les efforts de conception d'une infrastructure de modélisation et le développement de modèles pour les produits 3D Secure. Avant de rejoindre CA Technologies, il a travaillé pendant plus de 15 ans pour les sociétés de solutions d'analyse SAS, FICO et HNC, développant des modèles pour des produits de détection des fraudes par carte de paiement, de fraude à l'assurance, de fraude fiscale (pour des autorités d'état et fédérales), de lutte contre le blanchiment d'argent, de prévision des pertes de crédit, de gestion du

risque de marge d'intermédiation et d'évaluation du risque de crédit (pour des sociétés publiques et privées). Hongrui détient un doctorat en mécanique des fluides numérique et a travaillé quatre ans au Los Alamos National Laboratory, au sein de l'équipe de recherche sur la modélisation théorique et la modélisation informatique des écoulements turbulents. Il détient plusieurs brevets issus de ces travaux.

Kannan Shah travaille dans le domaine de la science des données et de l'analyse avancée depuis six ans. Recruté par CA Technologies en 2013, il a participé au développement de l'infrastructure de modélisation analytique et du premier modèle produit par l'équipe CA Data Science. Avant de rejoindre CA Technologies, il était Senior Staff Scientist auprès de SAS Institute, où il a développé des modèles et techniques statistiques et assuré l'assistance client pour la solution SAS Enterprise Fraud Management. Il a contribué au développement de modèles de détection des fraudes pour des systèmes de règlement par cartes de paiement, virements et transactions ACH déployés aux États-Unis, au Royaume-Uni, au Mexique et dans la région Asie-Pacifique. Kannan est titulaire de plusieurs brevets qui sont le fruit de son travail auprès de SAS. Il détient une maîtrise en ingénierie électrique de la Drexel University de Philadelphie. Au cours de ses études, il a notamment travaillé sur la détection et l'estimation, le traitement des signaux stochastiques, l'intelligence machine, la reconnaissance des schémas statistiques, les réseaux neuronaux, la théorie de l'information, l'analyse spectrale d'ordre supérieur, ainsi que la conception et la complexité conception des algorithmes.

1 Dans les régions où les titulaires de carte ont été informés que les indicateurs 3D Secure représentaient un gage de sécurité, l'affichage d'un message indiquant que la transaction est protégée par 3D Secure peut contribuer à les rassurer.

2 Le terme « truth data » fait référence aux informations sur le niveau de carte et la transaction qui identifient les transactions que le processus d'authentification doit interrompre.

CS200_94860_1014