Atelier 4 : DIGITAL ET KYC : DE NOUVEAUX RISQUES MAIS AUSSI DE NOUVELLES OPPORTUNITÉS

Intervenants :

Jérôme GRELIER
Managing Director - Financial Services - Accenture

Thierry GENEST
Directeur de projets chez CATS

Anne-Lise BUSCAYLET
Responsable du risque de criminalité financière pour le domaine banque de détail d' HSBC

Assurer la conformité des processus KYC nécessite de collecter et de fiabiliser de plus en plus de données, en maîtrisant l'augmentation des coûts tout en optimisant l'expérience client et les performances commerciales d'une banque.
L'objectif de cet atelier était de faire un zoom sur les cas d'application où le digital peut d'ores et déjà permettre d'automatiser une partie importante des processus KYC, tout en allant plus loin dans les contrôles qui sont réalisés aujourd'hui et en fluidifiant le parcours client.
Le digital englobe aujourd'hui beaucoup de définitions, concepts et technologies et peut avoir de nombreuses significations différentes. Dans le domaine du KYC, les principaux cas d'application déjà déployés au sein de l'Industrie Banque / Assurance sont les suivants :
Robotique : un premier levier pour gagner en efficacité et réduire les risques opérationnels, déployé généralement comme solution tactique et comme une première étape sur le chemin de la digitalisation ;
RAD / LAD / Contrôle d'Identité : des solutions de contrôle de documents devenues incontournables pour digitaliser les processus KYC, et une évolution des solutions vers le marché SaaS ;
Workflow / Orchestration de l'EeR : une gestion industrialisée du cycle de vie des clients corporate et une disruption du marché en 2017 par certaines Regtechs ;
Blockchain : une opportunité de partage du KYC pour un modèle « KYC Utility ».
L'IA et Adverse Media : de nouvelles capacités d'analyse, là encore proposées par des Regtechs, en temps réel et dans plusieurs dizaines de langues différentes des « negative news » afin d'assister les analystes KYC dans l'identification d'alertes pour une institution financière.
En illustration, le cas d'une grande banque de détail qui a digitalisé le processus d'entrée en relation et de KYC en agence. Le processus démarre par la prise de photos des documents du client par le conseiller avec une tablette, suivi par l'automatisation des contrôles sur les différentes bases externes et l'ouverture du compte en quelques minutes. Bien sûr cette automatisation quasi complète, garantissant par ailleurs la conformité vis-à-vis des différentes réglementations, vise la grande majorité des clients qui ont un risque faible et pour lesquels aucune anomalie ou suspicion n'est levée. Les risques élevés et les exceptions restent et resteront traités par des équipes spécialisées.
Le digital permet également aujourd'hui de résoudre les problématiques de revue périodique des KYC et des efforts de remédiation auxquels le secteur des services financiers fait face. Un autre retour d'expérience bancaire a été partagé illustrant la nécessité d'approches spécifiques et différentes par les risques, la possibilité de développement d'alertes automatiques pour les conseillers et les équipes KYC dédiées, le traitement automatique des documents existants ou reçus du client, la consultation automatique des bases externes et l'intérêt d'offrir au client la possibilité de fournir des informations et des documents par différents canaux (y compris depuis son smartphone).
Le digital présente encore des perspectives et comme dans beaucoup de domaines l'innovation permettra d'aller progressivement de plus en plus loin dans l'automatisation du KYC tout au long du cycle de vie des clients. Le digital devrait notamment permettre de viser à terme une « Compliance by Design » et un KYC dynamique, voire le développement significatif du marché des KYC Utilities qui jusque-là n'ont pas réussi à s'imposer et/ou la constitution de KYC Utilities internes au sein des grands groupes bancaires Internationaux. Mais les cas d'applications concrets du digital aboutissant à des résultats tangibles dans le domaine du KYC sont déjà nombreux aujourd'hui. Ces solutions sont complémentaires et peuvent se présenter sous forme de briques qu'il est possible d'assembler – à l'instar des Regtechs qui ne se positionnent généralement pas sur le processus KYC de bout en bout mais qui se spécialisent et offrent de nouvelles solutions sur une problématique spécifique.

2ème plénière / Clôture

PROSPECTIVE : CROISSANCE ÉCONOMIQUE SÉCURISÉE ET DIGITAL MAITRISÉ ?

Intervenants :

Bernard GEORGES
Direction des ressources et de l'innovation – SOCIÉTÉ GÉNÉRALE

Hélène LAVOIX
Directrice - The Red (Team) Analysis Society

Myriam QUEMENER
Magistrat,
Docteur en droit, Conseiller Juridique auprès de la Mission de lutte contre les cybermenaces

Anne SOUVIRA
Conseillere du Préfet de Police, Chargée de mission aux questions liées à la cybercriminalité

Jean-Michel HUET
Partner Africa and Internetional Development Bearing Point

Cette plénière de clôture intéressait différentes institutions publiques, notamment la Préfecture de police, la magistrature ; et privées par le biais du groupe Société Générale ; également, faire un parallèle avec le digital en Afrique pour comparaison avec la France.
A travers ces différents points de vus, l'objectif était de débattre sur les perspectives du numérique et de l'Intelligence artificielle.
Pour ce qui est de la Police, la prospective sera de signaler les fraudes au cartes bancaires, ces plaintes massives créaient une difficulté quant à la lenteur du processus de dépôt de plainte: Le numérique pourra répondre à cette difficulté.
Par ailleurs, la Magistrature considère qu'avec le contexte géopolitique actuel, les réponses face à la cybercriminalité se traduisent par la prévention, la réglementation, la conformité.
On a un arsenal juridique assez lacunaire, jusqu'à la venue du RGPD: on veut renforcer la responsabilité des acteurs quant à leur système d'informations.
L'IA a pénétré notre monde en profondeur: l'IA devient une composante de la puissance pour les pays comme pour les entreprises. Révolution pour les humains car c'est la première fois que l'on gère un gouvernement et des activités quasi-parfaites. C'est également un avantage pour les autorités politiques qui sauront saisir l'opportunité.
Par rapport à la transformation digitale en Afrique: il y a 15 ans de cela, le taux de pénétration de télécom en Afrique était de 2%. Aujourd'hui, il a augmenté à 65%. En France on l'a fait en 80 ans. Ce qui est intéressant au niveau de l'identité numérique, c'est que le paiement mobile répond aussi à la logique de la connaissance-client.
Au Kenya, 1/2 transactions ont désormais lieues sur smartphone. Il faut savoir que la circulation routière en Afrique est assez difficile, donc cette possibilité de paiement leur permet de ne pas se déplacer pour effectuer des dépenses. : c'est une véritable Révolution technologique.

Nous remercions :

ThreatMetrix The Digital Identity Company · FIDUCIAL · experian. · CLEVER COURTAGE · orange · AIG CEV · CyAN Cybersecurity Advisors Network · pwc · accenture High performance. Delivered. · TECHNOLOGIES & SERVICES · RESOCOM Know Your ID Customer · open-root · NUANCE · IBM · Gendarmerie Nationale · Mercatel · EUROPOL · optimind winter · conseil national du numérique · CNIL · ALLSET · AMRAE · QP · France Connect · BearingPoint · CCI PARIS ILE-DE-FRANCE · FRONTEX

15 mars 2018 - Maison de la Chimie - 28 bis, rue Saint-Dominique - 75007 - Paris (FRANCE)

6ème Forum Européen de lutte contre la fraude du 15 mars 2018

L'IDENTITÉ NUMÉRIQUE : NOUVEAUX DROITS ET RISQUES DÉVELOPPEMENT VERSUS PROTECTIONS ET RÈGLEMENTS

Programme :

ATELIER 1 :
L'individu face au développement du digital : mieux connaitre et mieux sécuriser le consommateur

ATELIER 2 :
La sécurisation digitale des informations des entreprises

ATELIER 3 :
La réalité de l'identité, « pierre angulaire » d'un digital sécurisé

ATELIER 4 :
Digital et KYC : de nouveaux risques mais aussi de nouvelles opportunités

Discours Marie Azevedo, Présidente de ResoClub

J'ai l'honneur de présider l'association Reso-Club qui a su anticiper les sujets d'actualités relatifs à l'identité et aux risques de fraudes. A cet égard, l'Europe en pleine transformation digitale a pour objectif de promouvoir le numérique, transformer nos usages, permettre une identité plus confiante et sécurisée.
Parallèlement, l'objectif de ce Forum est de poser le contexte en veillant à bien distinguer les 3 niveaux d'implication de l'identité numérique selon l'individu, l'entreprise et les collectivités publiques. La fraude identitaire constitue une première étape à la commission d'infractions plus graves.

3 NIVEAUX D'IMPLICATION DE L'IDENTITÉ NUMÉRIQUE SELON L'INDIVIDU, L'ENTREPRISE ET LES COLLECTIVITÉS PUBLIQUES

Elle est une réalité qui concerne tout à la fois l'Etat et les particuliers touchés par les conséquences des actions de groupes terroristes, d'organisations criminelles, de fraudeurs qui perturbent notre Etat de Droit notre économie. Personne n'est à l'abri du risque d'usurpation d'identité, c'est le cas de Sylvain, Nacer, Charly et bien d'autres puisque depuis plus de 15 ans ils mènent un lourd combat.
Justifier de son identité permet notamment l'ACCES aux services bancaires, aux aides sociales, aux services éducatifs, aux droits logement, à la libre-circulation etc.
Il convient de réussir à résoudre le paradoxe de la sécurisation de l'identité numérique qui est à la fois gage de liberté et une menace pour cette même liberté. Lorsque le contrôle à l'enrôlement est défaillant, les risques et les conséquences sont parfois irréversibles. Il convient de réussir à résoudre le paradoxe de la sécurisation de l'identité numérique qui est à la fois gage de liberté et une menace pour celle-ci. Lorsque le contrôle à l'enrôlement est défaillant, les risques et les conséquences sont parfois irréversibles. C'est une évidence économique, l'évolution du NUMÉRIQUE s'impose comme la tendance technologique la plus répandue sur les tous les secteurs d'activité. C'est le moment. L'identité numérique pose de multiples questions, il faut anticiper sur risques potentiellement irréversibles. Avant-hier, nous étions majoritairement déconnectés, notre identité semblait être protégée. Hier, nous étions tous connectés, notre identité était parfois dangereusement exposée.
Aujourd'hui, nous sommes dans l'hyperproximité, dans l'instantané, en mode nomade multicanal avec une réalité virtuelle ubiquitaire.
Dans ce monde-là, notre identité est, si nous ne mettons pas en œuvre des garde-fous, en réel danger.

ENJEUX DE LA TRANSFORMATION DIGITALE

1ère plénière / Introduction des débats

Le monde d'aujourd'hui évolue très vite, mais il faut se méfier des généralités car certains Etats avancent moins que d'autres.
L'Internet est l'outil qui permet de contrôler tout le monde mais jusque-là aucun Etat ne s'y intéressait réellement. Aujourd'hui, qui peut garantir la sécurité?
L'Etat se préoccupe désormais de la stratégie numérique : c'est devenu une affaire politique, il y a une prise de conscience sur les enjeux du numérique en France. L'Assemblée Nationale est de plus en plus impliquée : les politiques en matière de numérique pour nos emplois, sécurité, citoyens, passe par une conscience au niveau de l'Etat.
Dans le secteur public, on peut évoquer l'exemple de la Gendarmerie Nationale, qui effectue sa transformation digitale à l'image du secteur privé : La gendarmerie doit aussi se préparer aux travaux de demain puisque la technologie ne va pas s'arrêter là, c'est une réalité juridique. Les gendarmes changeront de métier, on ne parle plus du gendarme 30 ans avant, c'est une nouvelle vision du gendarme moderne.
Ensuite, sur l'inclusion numérique, il y a une prise de conscience mais chaque collectivité territoriale met en œuvre de manière différente. On peut déclarer les impôts en ligne, mais les gens ne savent pas faire,
Le digital est une chance comme un risque. Les enjeux de la transformation digitale couvrent l'ensemble des acteurs, que ce soit du service public ou privé.
La révolution digitale est au cœur de notre stratégie, qui n'est pas simplement technologique mais engendre une véritable transformation du processus: risque menace et risque opportunité.
Quels sont les risques opérationnels ? Fraude? Cyber risque?
En entreprise, il y a 3 niveaux: l'Identité numérique de ses fournisseurs, collaborateurs et clients. Et comme partout, il y a des opportunités et des risques menaces. L'identité numérique permet d'avoir une meilleure connaissance de son client. Egalement, Il y a des menaces liées à la cybersécurité, il faut mettre en place des outils techniques et de sensibilisation (RGPD) qui certes va représenter un poids pour l'entreprise, il y a donc un travail collaboratif à réaliser.
été détectés, qui proposent des impôts et taxes à la carte.
La lutte contre la cybercriminalité du Parquet de Paris représente 1700 affaires en 2 ans. 40% des dossiers sont des fraudes hors du territoire national.
L'internationalisation rend difficile la lutte, il est nécessaire de renforcer la réciprocité entre les différents pays et notamment avec USA.

Intervenants :

Serge MAGDELEINE
Directeur Général de Crédit Agricole Technologies et Services et Directeur des Parcours Digitaux Groupe de Crédit Agricole SA
Président d'Honneur du 6ème Forum

Laure de la RAUDIÈRE
Député d'Eure-et-Loir à l'Assemblée Nationale et membre de la Commission de réflexion sur le droit et les libertés à l'âge du numérique

Louis POUZIN
Ingénieur informatique

François MALAN
Risk Manager et Vice-Président de l'AMRAE

Eric FREYSSINET
Chef de la Mission Numérique de la Gendarmerie Nationale

Atelier 1 : L'INDIVIDU FACE AU DÉVELOPPEMENT DU DIGITAL : MIEUX CONNAITRE ET MIEUX SÉCURISER LE CONSOMMATEUR

Intervenants :

Lionel FOUILLEN
Business Developer FRANCE CONNECT chez SGMAP/DINSIC

Jean-Christophe LE TOQUIN
Président de CyAN, Président Fondateur etde SOCOGI, société de conseil en affaires publiques pour les entreprises de technologies et de cybersécurité

Philippe MAZURIER
Directeur du développement Fraude et ID, Europe du Sud - EXPERIAN

Jean-Michel CHANAVAS
Délégué Général - Mercatel

Parler identité numérique, passe d'abord par une définition de l'identité : Caractère de ce qui est identique (similitude parfaite) ou ce qui détermine une personne ou un groupe (deux aspects divers d'une réalité unique) ou données qui déterminent chaque personne et qui permettent de la différencier des autres (Ensemble des données de fait et de droit qui permettent d'individualiser quelqu'un (date et lieu de naissance, nom, prénom, filiation, etc.). Autant de representation pour une même définition.
Afin d'assurer la qualification d'un client, nous pouvons prendre en compte différentes autres notions qui viennent caractériser celui-ci :
• Identité Administrative (délivrée par une autorité ayant capacité à enregistrer et assurer l'existence d'une personne suite à déclaration préalable)
• Identité Biométrique (identifier une personne à partir de données biologiques ou comportementales)
• Identité connectée (identité permettant de se connecter à des médias digitaux, peut être différente des autres : alias, avatar, mèl, pseudo, représentation de soi)
• Identité mémorisée (capacité de la mémoire informatique à tracer une personne, question sur droit à l'oubli avec médias numériques ?).

Renforcer l'efficacité de la qualification des prospects ou des clients passe par la réalisation d'un environnement complet, mais celui-ci est conditionné par un cadre réglementaire favorable au croisement de données (data analytics, intelligence artificielle) et à l'approche collective en vue de lutter contre la fraude et à la protection renforcée des consommateurs.

Atelier 2 : LA SÉCURISATION DIGITALE DES INFORMATIONS DES ENTREPRISES

Intervenants :

Gwendal LEGRAND
Directeur des technologies et de l'innovation chez CNIL

Dan CHELLY
Directeur associé, conseil et gestion des risques - OPTIMIND WINTER

Sandrine CULLAFFROZ-JOVER
Avocat, Directeur chez PwC Société d'Avocats

Agnieszka BRUYÈRE
Directrice Sécurité chez IBM France

Joël THIERY
Elu de la Chambre de Commerce et de l'Industrie, Référent «Intelligence économique & Cybersécurité»

Cet atelier a eu pour objectif de mettre en perspective les différents aspects de la sécurisation digitale des informations des entreprises dans 5 directions :
- la sécurisation globale du patrimoine informationnel et la gestion des risques à travers un exposé de Dan Chelly sur la gouvernance et le respect des règles de gestion des risques (équilibre entre les chances de gagner et les risques de perdre) ;
- la sécurisation des droits des personnes dans la collecte et le traitement des données les concernant à travers un exposé de Gwendal Legrand (équilibre entre les droits des personnes et le développement du Big Data et du KYC) ;
- la sécurisation juridique du patrimoine des entreprises autour du secret d'affaires, de la propriété intellectuelle et industrielle, ou financières à travers un exposé de Sandrine Cullaffroz-Jover (équilibre entre la protection du business et la liberté des affaires) ;
- la sécurisation technique des systèmes d'information face au développement de la fraude et de la cybercriminalité à travers un exposé d'Agnieszka Bruyère (équilibre entre l'ouverture des systèmes et leur sécurisation et importance de la continuité d'activités) ;
- la sécurisation de l'intelligence économique et la préservation de nos savoirs à travers un exposé de Joël Thiery, membre élu de la CCI Paris Île-de-France, référent "Intelligence économique et cybersécurité" (équilibre entre partage d'informations et protection des secrets).
L'ambition de cet atelier a été de montrer la complémentarité des approches des intervenants et la nécessité de travailler ensemble à la recherche de l'équilibre entre les objectifs de développement et les contraintes de conformité auxquels sont confrontées les entreprises.

DÉDICACES OUVRAGES AVEC LES AUTEURS :

« LUTTER EFFICACEMENT CONTRE LA FRAUDE »
« ON A VOLÉ MON NOM ! »

Atelier 3 : LA RÉALITÉ DE L'IDENTITÉ, « PIERRE ANGULAIRE » D'UN DIGITAL SÉCURISÉ

L'identité numérique correspond à l'ensemble des informations que l'on peut trouver sur une personne via internet. Avec le développement d'internet et notamment de la diversité des réseaux sociaux, la gestion de l'identité numérique devient un enjeu majeur : l'objectif est de limiter les risques et les dérives tels que l'utilisation des données à des fins frauduleuses, (quid de l'usurpation d'identité).
Comment appréhender les nouvelles escroqueries à l'identité numérique ?
Pour détecter la fraude, l'agence Frontex contribue à harmoniser les contrôles aux frontières au sein de l'UE.

RESOCOM TRAITE PLUS DE 2 MILLIONS DE DOCUMENTS D'IDENTITÉ PAR AN

Elle va exercer son contrôle sur la personne par la technique du Profilage : au regard du comportement de l'individu, sa nationalité, sa tenue vestimentaire car celle-ci peut être trompeuse : pour exemple, une personne va s'habiller exactement de la même manière que la photo utilisée sur le passeport : cela évoque une suspicion certaine.
ThreatMetrix est le spécialiste de l'identité numérique, il fournit une plateforme intégrale pour les renseignements sur l'identité numérique et l'authentification. Leurs solutions reconnaissent jusqu'à 95 pour cent des visiteurs retournant sur le site. Ils détectent instantanément les transactions à haut risque et les évaluons d'une façon dynamique, ce qui permet aux entreprises numériques de développer leur chiffre d'affaires en ligne en toute sécurité et de personnaliser l'expérience numérique des clients de confiance.
Ensuite, l'AIGCEV (Association Internationale de Gouvernance du Cachet Électronique Visible). Le Cachet Électronique Visible (CEV) est un dispositif qui, s'appuyant sur une signature électronique, garantit l'origine et l'intégrité des données clés d'un document, quel que soit le support, électronique ou papier. Le CEV nécessite un écosystème de confiance, écosystème administré par l'AIGCEV (cf. détails sur aigcev.org). Plus d'une dizaine de cas d'usage sont maintenant effectifs dont les Justificatifs de domicile, les Vignettes Crit'Air, les Bulletins de salaire ou encore les Diplômes, et bientôt les Relevés d'Identité Bancaire.

Depuis bientôt 20 ans, la société RESOCOM se consacre à l'expertise de documents d'identité et administratif au niveau international. Elle met en œuvre des techniques de RAD / LAD et analyse plus de 2,5 millions de documents chaque année, fournissant à ses clients à une expérience riche et leur donnant accès à des bases de données mutualisées.
ResoCom lance 2 nouveaux produits, un pour capturer et reconnaître automatiquement un document à partir d'un mobile et un autre pour traiter les dossiers depuis leur complétude jusqu'à l'analyse croisée des informations.

Intervenants :

Jérémy SOUCHET
Centre d'excellence de lutte contre la fraude documentaire de l'agence - FRONTEX

Gilles BOISAUBERT
Directeur des opérations - RESOCOM

Gilles BARRÉ
Président Fondateur d'AIGCEV - Le Cachet Électronique Visible (CEV)

Alain CHLON
Chargé de la commercialisation des services de ThreatMetrix

Jean-Paul PINTE
Expert scientifique - CSFRS, membre expert AILCC