



Le maillon le plus
faible est
l'utilisateur :
le conseiller,
son client ou
le développeur
du système
informatique.

GÉRARD BÉRUBÉ

DEVANT LES RISQUES accrus de vol d'identité et l'interrogation persistante axée sur la valeur de la signature et du consentement électroniques, les autorités réglementaires insistent sur la fiabilité de l'identification, qui dépasse le simple mot de passe et l'autorisation par courriel.

Dans le traitement de réclamations en assurance comme dans l'univers transactionnels des valeurs mobilières, le lien est de plus en plus électronique entre l'institution, le client et l'intermédiaire. La raison officielle invoque les impératifs environnementaux, mais essentiellement pour des questions de productivité et de réduction des coûts, les transactions sans papier sont devenues un outil de développement prioritaire des institutions financières. Les questions portant sur la sécurité et sur la conformité revêtent donc une importance cruciale.

Un récent article de *Conseiller.ca*, relatant qu'un nombre record de délits économiques avaient été perpétrés au Canada en 2009, a souligné qu'à « l'échelle mondiale, ce sont les firmes de communication, d'assurance, de services financiers, d'hôtellerie et de loisirs qui sont les plus susceptibles d'être l'objet d'un délit économique ». La nature des produits et services offerts par l'industrie des services financiers attire le fraudeur.

Transactions mobilières sans papier

ÉVITER LES BRÈCHES DE SÉCURITÉ

Les traitements et transactions sans papier se multiplient, rendant la relation client-conseiller-institution financière toujours plus informatisée. Cette plus grande fluidité et cette transparence n'est pas sans alimenter des préoccupations relatives à la sécurité ni sans rappeler le conseiller à ses obligations en matière de conformité.

UNE MENACE BIEN RÉELLE

L'enjeu est donc réel, sans toutefois trop préoccuper les agences d'encadrement, qui ont plutôt tendance à s'en remettre à l'industrie. Du moins, à l'Autorité des marchés financiers (AMF), le porte-parole Sylvain Théberge souligne l'implication de son institution dans les campagnes de sensibilisation et de prévention, notamment contre le vol d'identité et l'hameçonnage. Vincent Pâquet, conseiller aux Communications et aux relations de presse à la Chambre de la sécurité financière (CSF), indique pour sa part que son organisme ne dispose pas de réglementation particulière sur le sujet; il n'a que des dispositions générales sur la protection des renseignements personnels.

Sur le terrain, Richard Giroux, président du cabinet Option Fortune, résume que dans cette relation à trois, il est du ressort et de la responsabilité de l'institution d'offrir un système sécurisé alors que le respect de la conformité est l'affaire du conseiller. Quoiqu'il en soit,

«on ne peut rien faire, même un simple changement d'adresse, sans autorisation signée du client. On ne prend également ni ordre ni confirmation par courriel. Notre assurance-responsabilité ne nous le permettrait pas. À la limite, une confirmation signée transmise par télécopieur sera acceptée, mais encore, certaines institutions ne veulent pas un document numérisé.»

Richard Giroux insiste toutefois sur l'importance pour le conseiller d'être vigilant. Stephen Lingard retient également cet impératif de vigilance. Le spécialiste de la protection des renseignements personnels sur les formulaires électroniques à la Coalition canadienne contre la fraude à l'assurance observe une corrélation très étroite entre l'accroissement des transactions électroniques et l'augmentation des fraudes. «En matière de protection des renseignements personnels, on ne saurait trop insister sur la vérification de l'identité de la personne avec qui le conseiller fait affaires. Que ce soit par un contact en

personne ou par téléphone, une double vérification peut être utile dans le cas d'une transaction électronique.»

Dans le domaine du risque, une grande distinction sépare le monde de l'assurance de l'univers des produits et services bancaires et financiers. «La nature de ces industries est différente, résume Stephen Lingard. En assurance, la fraude va généralement affecter les réclamations. La signature électronique n'est pas un enjeu majeur ici. Et ces réclamations sont suivies d'une vérification personnelle, notamment dans le cas de dommages à la propriété ou au véhicule automobile. Dans les domaines bancaires et financiers, les attaques et tentatives de fraude visent davantage le vol d'identité ainsi que l'accès au compte de banque et aux renseignements personnels de l'individu.»

Luc Poulin, conseiller principal en sécurité pour l'Institut de sécurité de l'information du Québec (ISIQ), ne peut chiffrer la fréquence des tentatives de fraude. «Il n'y a pas de loi forçant la

divulgaration des attaques. Mais une chose est sûre: le recours aux formulaires électroniques expose à de nouveaux risques, ouvrent de nouvelles portes sur le système des institutions financières.

contexte d'affaires et alors que l'encaissement légal est en train de s'adapter, la relation électronique devrait comprendre un processus de validation de la transaction.

du commerce des valeurs mobilières (OCRCVM). Le problème de sécurité demeure réel, et la question de la signature électronique est des plus pertinentes. «Du moins, c'est une question que se posent de plus en plus les conseillers. Comment fait-on pour valider?» M^{me} Crépin donne l'exemple des difficultés et des limites éprouvées dans l'exercice du vote électronique pour illustrer que tout n'est pas sans faille. «La jurisprudence accepte la validation par télécopieur, sans l'original. Mais nous n'allons pas jusqu'à accepter qu'une transaction soit validée par courriel. Il faut une communication directe avec le client. Il faut lui parler.»

Le cadre légal actuel s'inspire de la révision de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* lancée en mai 2002. Par cet exercice, le législateur apportait un certain nombre de changements aux règles qui prévalaient alors en matière d'identification et de vérification d'identité des clients. Il proclamait également l'obligation de mettre en œuvre un programme de conformité.

LA SIGNATURE ÉLECTRONIQUE

Cette révision comportait un chapitre sur la détermination de l'identité du tiers, lorsque le compte est destiné à être utilisé par le tiers ou en son nom. Un autre chapitre était consacré à l'identification et à la vérification d'identité de particuliers. Le législateur a réitéré l'obligation pour le membre «d'obtenir la fiche-signature, la convention de tenue de compte ou la demande d'ouverture de compte qui porte la signature de toute personne autorisée à donner des instructions à l'égard du compte de la personne physique». Et il introduit le concept de signature électronique, «désormais assimilée à la signature».

Dans un bulletin daté du 18 novembre 2002, l'OCRCVM y faisait écho

« Plus on migre vers les relations électroniques entre conseiller et client, plus le danger s'accroît. »



Carmen Crépin, vice-présidente pour le Québec, OCRCVM

Si ce système est mal développé, mal protégé, il devient possible d'avoir accès à l'information.» Mais l'on parle d'un risque accru pour l'institution qui peut cependant devenir acceptable lorsqu'il est mis en relation avec les gains dont celle-ci bénéficie.

L'ERREUR EST HUMAINE

L'analyse du risque repose sur une approche systémique personne-processus. «Le maillon le plus faible est la personne, que ce soit l'utilisateur (le conseiller, le client) ou celui qui développe le système. Vient ensuite le processus. Lorsque l'électronique est introduite, le processus change. Si elle n'est pas adaptée, il peut en résulter une problématique de sécurité, de validation ou de vérification.» Luc Poulin rappelle que les contrats électroniques existent depuis longtemps et qu'à l'origine, ils reposent sur une entente de gré à gré. Mais avec l'évolution du

Le spécialiste de l'ISIQ ajoute à l'équation les choix technologiques. «La technologie elle-même entraîne son lot de de risques.» Surtout, dit-il, la technologie n'est pas une panacée. Elle peut créer une illusion de sécurité. «La technologie dit que le "conduit" est sécurisé entre l'institution et l'utilisateur. Elle ne dit pas si les données sont en sécurité.» Dans la foulée, Luc Poulin souligne qu'en matière de délits économiques, la fraude électronique impliquant le vol d'argent est plutôt rare. «Ces transactions laissent toujours des traces informatiques.» Les attaques visent donc essentiellement les bases de données.

UNE DIFFICILE VALIDATION

Sur ce dernier point, Carmen Crépin se veut plus directe encore. «Plus on migre vers les relations électroniques, plus le danger s'accroît», résume la vice-présidente pour le Québec de l'Organisme canadien de réglementation

en annonçant permettre désormais l'utilisation de signatures électroniques ou numérisées lorsqu'une signature est requise relativement à des conventions, des opérations ou des contrats conclus, entre autres, avec ou entre le membre et ses clients. On retenait qu'il existait plus d'une façon de signer et de donner effet à un document.

Mais l'organisme d'autoréglementation rappelait, du même coup, les

dépend des possibilités du système technologique employé par le membre. «Entre autres exigences technologiques, il faut veiller à ce que le système garantisse la non-répudiation, c'est-à-dire que le signataire ne puisse pas répudier sa propre signature sur un document ou relativement à un document», peut-on lire dans le bulletin.

Sur ce point, l'Association exige de ses membres qu'ils obtiennent une opinion juridique fiable attestant que la technologie et le système employés

Bien que la législation ne définisse pas le mode de consentement requis, elle prévoit néanmoins un consentement tacite. «On parle de consentement tacite. Mais personnellement, je ne m'appuierais pas nécessairement là-dessus», commente Carmen Crépin.

En outre la plupart des lois provinciales précisent qu'une signature électronique ne doit pas nécessairement ressembler à une signature «physique» pour être valide et exécutoire. Par exemple, la signature peut être un code, un son ou tout autre symbole, et peut faire partie intégrante du document signé ou être séparée du document, tant que son association avec le document peut être établie de façon claire. «Il est ici question d'une identification fiable. À notre avis, un simple mot de passe ne suffit pas nécessairement. Et dans le cas d'une confirmation de transaction, on va accepter une télécopie signée, mais certainement pas un courriel», renchérit Carmen Crépin.

Dans son interprétation, l'Association ajoute qu'il ne semble pas y avoir de restrictions ni de limitations à l'usage de signatures électroniques pour la formation et l'effet de contrats électroniques. «Tant qu'on peut établir l'association entre la signature électronique, la personne et le document, et tant que l'intention de signer est démontrée, la signature électronique ainsi utilisée est considérée comme valide.»

Ces précisions étant, il revient au conseiller d'être vigilant et conscient du danger du vol d'identité et de fausse signature ou représentation. Carmen Crépin tient également à lui rappeler qu'il ne peut modifier unilatéralement les renseignements relatifs à son client sans l'autorisation de ce dernier, et que le fichier-client devrait être mis à jour au moins une fois l'an. «C'est une obligation du conseiller, mais aussi une responsabilité du client.»



Rendre conforme un document électronique

LA LOI PRÉVOIT, entre autres exigences, qu'un document ou des renseignements sous forme électronique doivent :

- être accessibles par l'autre personne de manière à être utilisables pour consultation ultérieure;
- être conservés par l'autre personne;
- être présentés de la même manière ou essentiellement de la même manière que sous la forme non électronique précisée.

Surtout, il faut que :

- la signature électronique permette d'identifier la personne de façon fiable;
- l'association entre la signature électronique et le document électronique pertinent soit fiable.

«Ainsi, en ce qui concerne les deux derniers points, la simple acceptation d'un message électronique par un client ou l'utilisation par un membre d'un site Web protégé par un mot de passe ne constituent pas des solutions qui satisfont aux exigences», insiste-t-on.

exigences légales et la définition juridique de la signature, inspirées des lois sur le commerce électronique en vigueur dans les provinces et territoires. Sur cet aspect, le Québec, avec sa *Loi concernant le cadre juridique des technologies de l'information* (et l'article 2827 du Code civil), a joué le rôle de pionnier. On insistait aussi sur le fait que l'utilisation de signatures électroniques

pour les signatures numériques satisfont aux exigences des lois applicables dans les provinces ou territoires où ils sont censés être utilisés. «Un membre peut présenter sa propre opinion juridique ou l'opinion juridique d'un organisme de certification.»

Il est également rappelé que le membre doit obtenir un consentement avant d'utiliser une signature électronique.