CLASSESAFFAIRES
ACTUALITÉS ▪ SÉMINAIRES ▪ PERSPECTIVES

Blakes
AVOCATS CANADIENS

TENDANCES

TECHNOLOGIE

D'ici la fin de 2016 et en 2017, nous présenterons un aperçu des tendances actuelles dans divers secteurs. Le premier article de notre série porte sur la technologie, particulièrement les technologies financières (les « fintech ») et la cybersécurité.

1

Prêts entre particuliers : à quoi les fintech doivent-elles s'attendre au Canada?

Il est à prévoir que d'autres mesures législatives visant les fintech feront leur apparition en 2017. En effet, l'étude de marché du Bureau de la concurrence du Canada à ce sujet, qui explore le besoin possible de réforme réglementaire pour promouvoir une plus grande concurrence tout en maintenant la confiance des consommateurs dans le secteur, devrait être publiée au printemps.

Des pays comme le Royaume-Uni ont déjà mis en place une réglementation des fintech encourageant l'innovation, en créant notamment un « centre d'innovation réglementaire », c'est-à-dire un espace sécuritaire où mettre à l'essai des produits et services financiers novateurs sans craindre les représailles réglementaires. L'Australie et la Chine ont proposé des approches semblables pour le secteur.

À l'instar de ces pays, le Canada est perçu comme une plaque tournante des fintech à l'échelle mondiale, grâce à ses d'institutions financières nationales renommées ayant été parmi les premières à lancer des projets relatifs à la technologie des chaînes de blocs et aux nombreuses jeunes entreprises de fintech qui émergent dans les grandes villes. La réglementation ne suit cependant pas le même rythme.

En septembre, la Commission des valeurs mobilières de l'Ontario (la « CVMO ») a franchi une nouvelle étape en décidant d'autoriser l'inscription à titre de courtier sur le marché dispensé d'un prêteur en ligne, Vault Circle Inc. Il s'agit d'un pas important pour les plateformes de prêts entre particuliers en Ontario, qui sont actuellement assujetties à une réglementation sur les valeurs mobilières très stricte. Grâce à ce titre, Vault Circle Inc. dispose désormais de l'approbation réglementaire lui permettant de participer au marché des investisseurs qualifiés.

Cette annonce a été suivie, en octobre, par l'inscription pancanadienne à titre de courtier d'un autre prêteur en ligne, Loop Securities Inc., qui se prévalait d'une dispense pour placement au moyen d'une notice d'offre très personnalisée.

Et pour la suite? La prochaine année nous dira si le Canada continuera à faire preuve de prudence ou encouragera les innovations qui ont le potentiel de transformer le secteur des services financiers.

2

Protection et sécurité des données

La croissance rapide des sociétés de fintech doit être équilibrée par une approche cohérente en matière de protection et de sécurité des données.

De par leur nature, les sociétés de fintech détiennent des données qui sont souvent des renseignements personnels à caractère très délicat, dont la date de naissance, le numéro d'assurance sociale, des détails concernant un compte bancaire, des justificatifs bancaires en ligne et le pointage de crédit. Pour une société de fintech relativement jeune, toute atteinte à la protection des données pourrait avoir un effet dévastateur sur la confiance des consommateurs et des investisseurs.

Les sociétés de fintech sont également confrontées à des défis en matière de protection de la vie privée lorsqu'elles étendent l'offre d'un produit ou d'un service mis au point pour un territoire précis à un autre territoire ayant des règles différentes en matière de protection de la vie privée et des données. Par exemple, lorsqu'ils sont offerts au Canada, nombre d'offres de produits et services américaines doivent être modifiées afin de tenir compte de la définition plus large du terme « renseignements personnels » au Canada.

Néanmoins, les questions relatives aux données et à la protection de la vie privée créent de véritables occasions pour les nouvelles sociétés de fintech. De fait, celles-ci pourraient avoir un avantage significatif par rapport aux fournisseurs de services financiers existants, car elles peuvent intégrer des mesures de protection de la vie privée et de sécurité à mesure que la technologie évolue, plutôt que de devoir les ajouter rétroactivement à des processus et des systèmes existants.

Pour en savoir davantage, consultez *Qui dit données, dit risques – Conseils en matière de sécurité et de protection de la vie privée pour les fintech.*

3

Voici le cyberdénonciateur

Avec une moyenne des coûts de plusieurs millions de dollars par atteinte à la protection des données, il ne sera pas surprenant de voir de nombreuses entreprises mettre l'accent sur la cybersécurité au cours de la prochaine année. Toutefois, les coûts liés à la cybersécurité pourraient être plus élevés que ce que prévoient ces entreprises, en raison des mesures législatives sur la dénonciation récemment présentées.

Le programme de dénonciation de la CVMO prévoit que les dénonciateurs pourraient se voir accorder des récompenses pécuniaires pouvant atteindre 5 M$ CA pour les renseignements qu'ils fournissent à la CVMO au sujet d'infractions aux lois sur les valeurs mobilières. La politique prévoit le versement de récompenses pouvant atteindre 1,5 M$ CA, même lorsque la CVMO n'a recouvré aucuns fonds auprès des contrevenants. La politique n'oblige pas les dénonciateurs à recourir aux mécanismes internes de signalement disponibles.

Cela pourrait avoir des répercussions importantes sur la cybersécurité pour les entreprises en Ontario. Par exemple, une société qui a émis des titres auprès du public (un « émetteur assujetti ») est tenue en vertu de la réglementation sur les valeurs mobilières de déclarer tout changement important, comme un changement dans ses activités commerciales, son exploitation ou son capital dont il est raisonnable de s'attendre qu'il aura un effet appréciable sur le cours ou la valeur de ses valeurs mobilières.

Si une atteinte à la protection des données entraîne un tel changement pour un émetteur assujetti et qu'elle n'est pas déclarée, un cyberdénonciateur pourrait signaler l'infraction directement à la CVMO et recevoir une importante récompense en argent en échange.

Il est donc essentiel que les entreprises en Ontario connaissent à la fois les bonnes façons de protéger leurs données et les répercussions qu'une cyberdénonciation pourrait avoir sur leurs activités.

4 L'offensive – la meilleure stratégie défensive?

Les contre-mesures offensives servent à inverser les rôles lors d'une cyberattaque, notamment en permettant à une entreprise d'identifier l'origine de l'attaque et de récupérer les données qui lui ont été volées (*hacking back*).

À titre d'exemple, il est possible de photographier le pirate à l'aide de la caméra de son propre système, de désactiver ou de détruire physiquement l'ordinateur ou le réseau du pirate, ou de recueillir des renseignements en implantant un maliciel dans le réseau du pirate.

Par définition, les contre-mesures offensives sont une stratégie à risque élevé. Parmi ces risques, on trouve la possibilité qu'une entreprise vise involontairement des personnes innocentes, car les pirates passent souvent par des tiers innocents pour masquer leur identité, ou s'attire des représailles de la part du pirate, ce qui pourrait empirer l'atteinte à la protection des données qui a déjà eu lieu.

Par ailleurs, ces mesures présentent de nombreux risques juridiques, notamment des violations possibles du *Code criminel*, de lois comme la *Loi canadienne anti-pourriel* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (loi fédérale sur la protection de la vie privée applicable aux sociétés du secteur privé) de même que des poursuites civiles.

Cependant, le droit applicable aux contre-mesures offensives est en constante évolution. En l'absence de décisions portant sur les enjeux mentionnés ci-dessus, il est impossible de savoir de quelle façon certaines dispositions possiblement pertinentes seront appliquées et comment les plaintes pour délit d'intrusion dans l'intimité seront traitées.

Pour en savoir davantage, communiquez avec Sunny Handa ou un autre membre de notre groupe Technologie.

Blakes