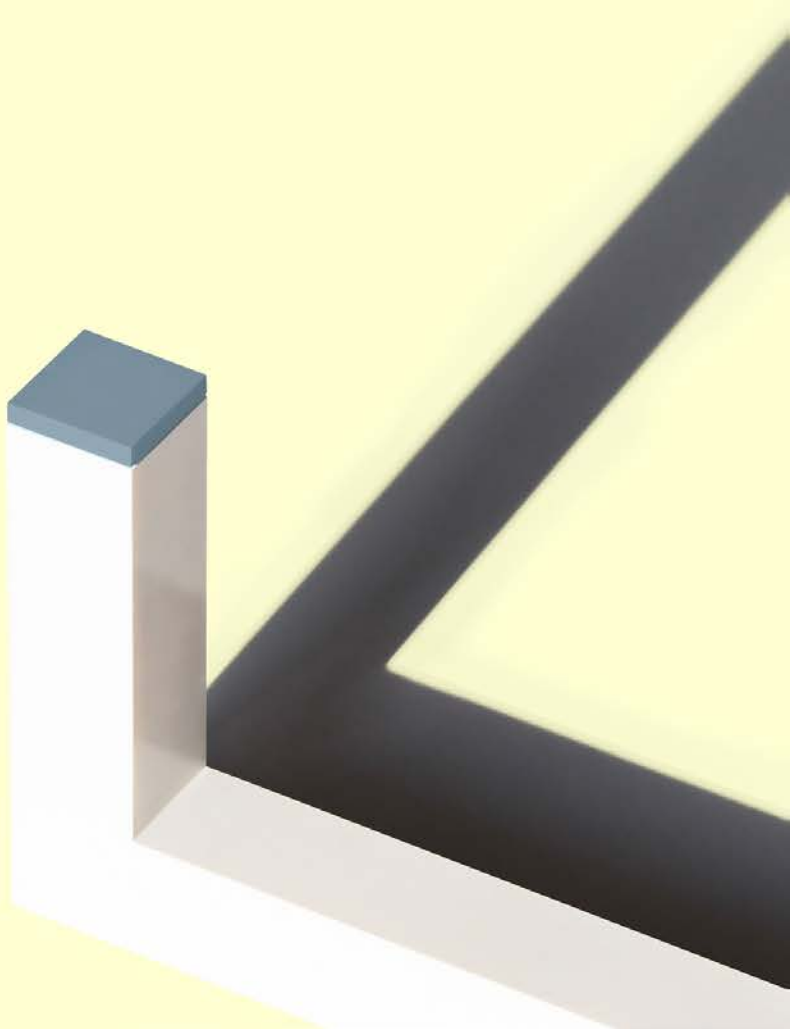
LANGLOIS

AVOCATS - LAWYERS

Les étapes d'un incident de sécurité dans une perspective juridique

Sécurité pour tous QUEBEC SEC

Jean-François De Rico



PLAN

Introduction

- Les sources
- Les catégories
- Les obligations

La qualification et les conséquences juridiques d’un incident de sécurité;

LES SOURCES

Information
Application générale
CcQ

Obligations contractuelles

Protection des renseignements personnels

Responsabilité civile

Règlements et normes sectorielles

Criminel

télécommunications

Loi concernant le cadre juridique des technologies de l'information

Loi sur la protection des renseignements personnels dans le secteur privé

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Loi sur la protection des renseignements personnels et sur les documents électroniques (PIPEDA)

Loi anti-pourriel

Loi sur le droit d'auteur

Code criminel

Code civil du Québec

Code de procédure civile

Lois sur les Sociétés

Recours extraordinaires

Jurisprudence

Lois et règlements d'application spécifiques….

Lignes directrices - Normes

Contrats

OBLIGATIONS

C onfidentialité

I ntégrité

A ccessibilité

Obligations	LOIS			
	LCCJTI	LPRPSP	LADOPPRP	PIPEDA
Préserver la confidentialité	25; 34	10	53	3, 4.7.1
Maintenir Intégrité	6, 19			
Assurer Accessibilité /disponibilité	19			
Appliquer mesures de Sécurité	25	10	63.1	4.7.1
1/3	26	17, 20	67.2, 70.1	4.1.3

LCCJTI / [C]-I-A

19. **Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et** de **l'utiliser aux fins auxquelles il est destiné.**

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LCCJTI / C-[I-A]

- 25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les **mesures de sécurité propres à en assurer la confidentialité**, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LCCJTI - Confidentialité

- 34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur **confidentialité doit être protégée par un moyen approprié au mode de transmission**, y compris sur des réseaux de communication.
- La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LPRPSP

- **10.** Toute personne qui exploite une entreprise doit **prendre les mesures de sécurité propres à assurer la protection des renseignements personnels** collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

LADOPPRP

63.1. Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

LPRPDE- ANNEXE 1

4.1 Premier principe — Responsabilité

4.1.3 Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.7 Septième principe — Mesures de sécurité

- Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1 Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.

4.7.2 La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis (…)

4.7.3 Les méthodes de protection devraient comprendre :

- **a)** des moyens matériels;
- **b)** des mesures administratives (autorisations sécuritaires/droits d'accès); et
- **c)** des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4 Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5 Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).

LPRPSP/ LADOPPRP 1/3

- **20.** Dans l'exploitation d'une entreprise, **un renseignement personnel n'est accessible**, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant ou **à toute partie à un contrat de service ou d'entreprise** qui a qualité pour le connaître **qu'à la condition que ce renseignement soit nécessaire** à l'exercice de ses fonctions ou à **l'exécution** de son mandat ou de son **contrat.**

67.2. Un organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme.

LPRPSP/ LADOPPRP 1/3

- **17.** La personne qui exploite une entreprise au Québec et **qui communique à l'extérieur du Québec** des renseignements personnels ou **qui confie à une personne à l'extérieur du Québec** la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer:
  1° que les renseignements **ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers** sans le consentement des personnes concernées **sauf dans des cas similaires à ceux prévus par les articles 18 et 23**;
  2° dans le cas de listes nominatives (…).

Si la personne qui exploite une entreprise **estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions** prévues aux paragraphes 1° et 2°, **elle doit refuser de** communiquer ces renseignements ou refuser de **confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser** ou de les communiquer pour son compte

70.1. Avant de **communiquer à l'extérieur du Québec** des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public **doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi**.

Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

LCCJTI – C-I-A

26. Quiconque confie un **document technologique** à un **prestataire de services** pour qu'il en assure la garde est, au préalable, tenu **d'informer** le prestataire quant à la protection que requiert le document en ce qui a trait à **la confidentialité** de l'information et quant aux **personnes qui sont habilitées** à en prendre connaissance.

Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que **les moyens technologiques** convenus soient mis en place pour en **assurer la sécurité, en préserver l'intégrité** **et, le cas** échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1

LOI SUR LE DROIT D'AUTEUR

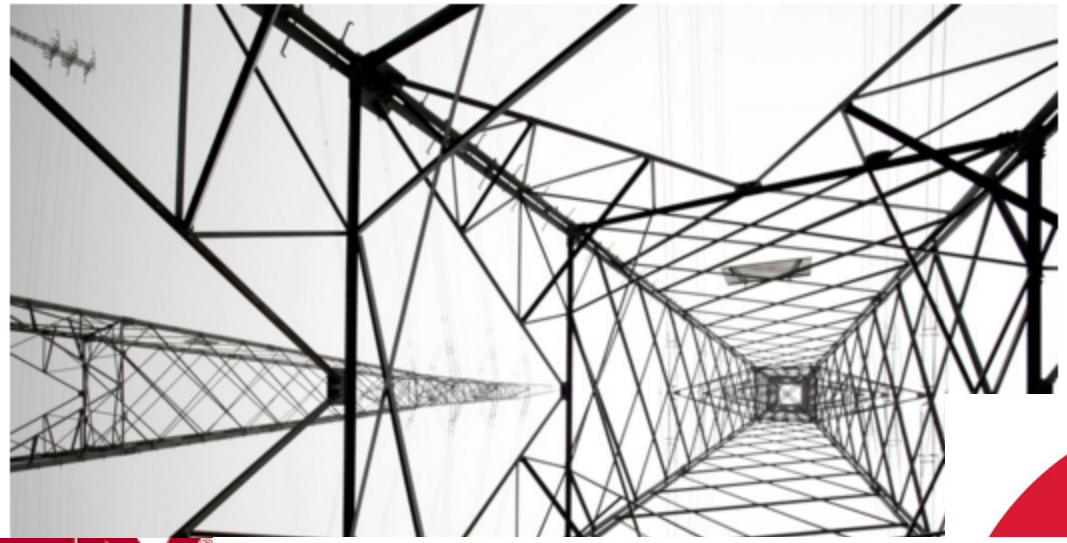
Interopérabilité (30.61)
Recherche sur le chiffrement (30.62)
Sécurité (30.63)

Ne constitue pas une violation du droit d'auteur le fait de reproduire une œuvre dans le seul **but d'évaluer la vulnérabilité d'un ordinateur, d'un système informatique ou d'un réseau d'ordinateurs ou de corriger tout défaut de sécurité**

-Doit donner au titulaire du droit d'auteur sur le programme un préavis suffisant faisant état de ceux-ci et de son intention de les rendre publics.

-Peut cependant les rendre publics sans préavis sil'intérêt du public d'être informé à cet égard l'emporte sur l'intérêt du titulaire de recevoir le préavis.

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



HOME DEPOT HACKED

56 MILLION CUSTOMER CREDIT & DEBIT CARD DATA EXPOSED

TJX THE T

T.J.maxx

Marshalls

HomeGoods

AJWright

Cost of data breach at TJX soars to $256m

Suits, computer fix add to expenses

The Boston Globe

By Ross Kerber, Globe Staff | August 15, 2007

TJX Cos. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

amsc

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (@0xcharlie)

Chris Valasek (cvalasek@gmail.com)

TÉLÉCOMMUNICATIONS XITTEL INC.

et

télécommunications Xittel

9116-6033 QUÉBEC INC., société légalement constituée faisant affaires sous le nom de **LES SYSTÈMES INFORMATIQUES CONCEPTA**

Demanderesses

c.

KEVIN COURTOIS

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data Security Breach Litigation This Document Relates to: All Financial Institutions Cases	MDL No. 14-2522 (PAM/JJK) **CONSOLIDATED CLASS ACTION COMPLAINT**

Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union, and First Federal Savings of Lorain, Individually and on behalf of a class of all similarly situated financial institutions in the United States,

Plaintiffs,

v.

Target Corporation,

Defendant.

JURY TRIAL DEMANDED

Portée et étendue de l'atteinte

Novembre et Décembre 2013	
Données de cartes de crédit /débit volées	**40 M**
Dossiers clients (nom – adresse - courriel – telphone)	**70 M**
Plus importantes brèche précédente en nombre de dossier (*record*)	90 million (TJ Maxx - 2007)

Target's Supplier Portal

LES ENTREPRISES QUI NOUS FONT CONFIANCE

Sélection - Encadrement des fournisseurs

LES ENT FAZIO FIANCE

MECHANICAL SERVICES

Sélection - Encadrement des fournisseurs

LES ENTRE FAZIO MECHANICAL SERVICES ONFIANCE

Malwarebytes

Citadel
Universal Spyware System

Sélection - Encadrement des fournisseurs

Processus d'approvisionnement et d'évaluation de risque de sécurité.	
	4.1.3 Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.
	LPRPSP 10. Toute personne qui exploite une entreprise doit **prendre les mesures de sécurité propres à assurer la protection des renseignements personnels** collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Segmentation des réseaux (Fournisseur vs POS)

Segmentation des réseaux accessibles aux fournisseurs des réseaux de transmission aux fins de vente Ou Processus d'authentification plus robuste (2FA)	
LCCJTI	25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les **mesures de sécurité propres à en assurer la confidentialité**, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.
PCI DSS	8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).

FAZIO MECHANICAL SERVICES

4.7 Septième principe — Mesures de sécurité

MÉTHODE DE PROTECTION

physique

processus / organisationnelle

technologique

sensibilisation / formation

LCCJTI - art 25

contrôle d'accès effectué au moyen

---procédé de visibilité réduite ou

---procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

PIPEDA annexe 1 , 4.7.3

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

Gouvernance

Responsabilité	Absence de responsabilité clairement attribuée
Système de gestion de la sécurité	Absence de contrôles Négligence dans le suivi

PIPEDA

4.7.1 Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.

4.7.2 La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis (…)

4.7.3 Les méthodes de protection devraient comprendre :

a) des moyens matériels;

b) des mesures administratives (autorisations sécuritaires/droits d'accès); et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

Gestion de l'incident et Notification

Target waited to comment on their breach until after it was announced by security blogger Brian Krebs. Then, the retail giant revealed in January that even more customers were affected than originally announced.

- **scrutinized** the Justice Department's information for three days to try and confirm the veracity of the U.S. officials' statements, thereby **allowing the data breach to continue for an additional three days**
- **attempted** to downplay the significance of the breach to avoid jeopardizing holiday sales
- **enticed** customers back to its stores by offering a 10% discount during the remaining holiday shopping days, with

However, the FTC pointed the finger at Wyndham's negligence in relation to security policies at the company's Phoenix data center—where the company stores and transfers data between its headquarters and its individual business units. As a result, Russian hackers managed to infiltrate its system and install phishing software on a myriad of Wyndham servers, gaining access to more than 500,000 customer accounts on three separate occasions between 2008 and 2010. Hackers then rang up more than $10.6 million in fraudulent credit card transactions, according to the suit filed in the U.S. District Court of Arizona.

But more troubling was that even after the company learned of the breach, it failed to take action to prevent it from happening again, according to the FTC's complaint, and as a result, the hackers were able to gain access on, not one, but two additional occasions. If Wyndham had added more complex user IDs and passwords, and made changes to software that was storing customer credit card data as unencrypted text, the company may have nipped the damage in the bud.

Gestion de l'incident et Notification

Principe fondamental :	Minimisation des dommages

NOTIFICATION OBLIGATOIRE EN CAS ATTEINTES AUX MESURES DE SÉCURITÉ (art. 10.1 LPRPDE)

10.1 **(1)** L'organisation déclare au commissaire toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu.

(…)

(3) À moins qu'une règle de droit ne l'interdise, l'organisation est tenue d'aviser l'intéressé de toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels le concernant et dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à son endroit.

ATTEINTES AUX MESURES DE SÉCURITÉ (art. 10.1 LPRPDE)

Avis relatif à une atteinte à toute autre organisation ou institution gouvernementale (art. 10.2)

Une organisation doit aussi aviser toute autre organisation ou institution gouvernementale capable de réduire le risque de préjudice pouvant résulter de l'atteinte ou d'atténuer ce préjudice

Registre des atteintes aux mesures de sécurité (art. 10.3)

Organisations doivent tenir et conserver un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion. Ces dossiers sont communiqués au commissaire sur demande.

Payment Card Industry Data Security Standards (PCI DSS) - twelve information security requirements.

Apply to all where cardholder data is stored, processed, or transmitted and require merchants like Target to:

- protect cardholder data,
- ensure the maintenance of vulnerability management programs,
- implement strong access control measures,
- regularly monitor and test networks, and
- ensure the maintenance of information security policies.

PCI Security Standards Council™

Traitement – conservation Données de paiement

The Minnesota's Plastic Card Security **Act.3 That statute provides:**	No person or entity conducting business in Minnesota that accepts a[] [credit or debit card] in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.
Recours collectif	The Court **CERTIFIES the following class under Fed. R. Civ. P. 23(b)(3):** All entities in the United States and its Territories that issued payment cards compromised in the payment card data breach that was publicly disclosed by Target on December 19, 2013.

In re: Target Corporation Customer Data Security Breach Litigation,

Plaintiffs are financial institutions that issue payment cards (…) Plaintiffs' customers used these payment cards to make purchases at Target stores during the period of the data breach in question.

Information (…) shows the data breach easily could have been prevented as Target failed to take adequate and reasonable measures to ensure its data systems were protected, ignored clear warnings that intruders had breached its systems, and failed to take actions that could have thwarted the breach.

Because of Target's numerous and preventable failures, Plaintiffs and the FI Class have suffered millions of dollars in damages

In re: Target Corporation Customer Data Security Breach Litigation,

Coûts

Coûts estimés pour les banques (ré-émission de 21.8 M de carte).	**200 million**s $
Règlements intervenus	$39 million avec les banques visées par le recours collectif $67 million avec VISA $10 million avec des clients

THE ALDO GROUP INC.
Plaintiff

v.

CHUBB INSURANCE COMPANY OF CANADA
Defendant

PCI Security Standards Council™

[18] This claim was asserted against Aldo by Moneris/MasterCard. Moneris/MasterCard allege that Aldo's failure to comply with PCIDSS and with its duty to reasonably safeguard customer-entrusted account data resulted in this ADC Event.

THE ALDO GROUP INC.
Plaintiff
V.
CHUBB INSURANCE COMPANY OF CANAD
Defendant

PCI Security Standards Council™

On March 31, 2011, MasterCard claimed that BMO, the bank involved in processing Aldo's Payment Card transactions, was responsible for its merchant (Aldo)'s non-compliance with PCIDSS. MasterCard informed BMO and Moneris accordingly

MasterCard threatened to impose an Assessment on Aldo for this breach of the PCIDSS. Based on the applicable Security Rules and Procedures (**Manual**), MasterCard assessed Aldo's overall financial liabilities at $US 4,884,128.13 in connection with this ADC Event. MasterCard indicated that Aldo's account could be debited by this amount.

Moneris forwarded this Mastercard letter to Aldo on April 1, 2011[17].

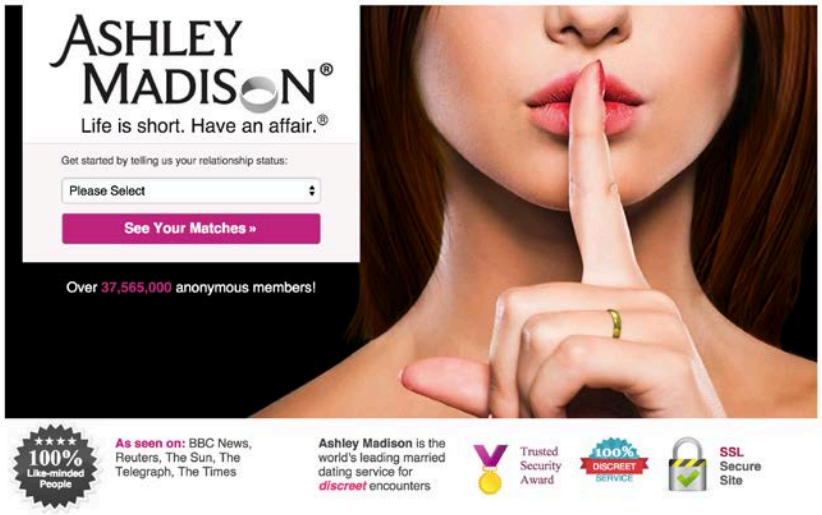
On April 18, 2011, MasterCard and Moneris debited Aldo's BMO accounts for USD$ 4.9 million (**Assessment**), allegedly pursuant to the terms of the Agreement.

Payment Card Industry Data Security Standards (PCI DSS) - twelve information security requirements.

Apply to all where cardholder data is stored, processed, or transmitted and require merchants like Target to:

- protect cardholder data,
- ensure the maintenance of vulnerability management programs,
- implement strong access control measures,
- regularly monitor and test networks, and
- ensure the maintenance of information security policies.

PCI Security Standards Council™



Rapport de conclusions d'enquête en vertu de la LPRPDE nº 2016-005

Ayant des motifs raisonnables de croire qu'une enquête devait être menée sur cette question et ayant compétence sur ALM, entreprise établie en Ontario, au Canada, le commissaire à la protection de la vie privée du Canada a pris l'initiative d'une plainte

Intensité des obligations

Questions :

L'organisation avait-elle un motif raisonnable pour conserver les renseignements personnels touchés par la brèche?

L'organisation conservait-elle les renseignements conformément à la *LPRPDÉ* et à la *PIPA*?

L'organisation avait-elle mis en place des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu'elle conservait?

Examen:

-Étendue et conformité de la conservation

-Mesures de protection de sécurité sans fil en place au moment de la brèche

-Mesures adoptées après l'incident

Facteurs considérés

Sensibilité de l'information	Compte tenu de la nature des renseignements personnels recueillis par ALM et du type de services qu'elle offrait, le niveau des mesures de sécurité aurait dû être très élevé, conformément au principe 4.7 de la LPRPDE. Lorsque l'on détermine si les mesures prises pour protéger les renseignements personnels étaient raisonnables dans les circonstances, il est utile de prendre en compte l'envergure et la capacité de l'organisation en question.
Taille de l'organisation	on ne peut s'attendre à ce qu'elle ait des cadres de conformité documentés comparables à ceux d'une grande organisation plus complexe. Une série de facteurs dans les circonstances actuelles indiquent qu'ALM aurait dû mettre en place un vaste programme pour assurer la sécurité de l'information: •la quantité des renseignements personnels détenus par l'entreprise, •la nature de ces données, •les répercussions prévisibles pour les utilisateurs du site en cas de piratage de leurs renseignements personnels et •les affirmations faites par ALM à ses utilisateurs concernant la sécurité et la discrétion.

Questions :

L’organisation avait-elle un motif raisonnable pour conserver les renseignements personnels touchés par la brèche?

L’organisation conservait-elle les renseignements conformément aux exigences de la loi

L’organisation avait-elle mis en place des mesures de sécurité raisonnables afin de protéger les renseignements personnels qu’elle conservait?

Examen:

-Étendue et conformité de la conservation

-Mesures de protection de sécurité sans fil en place au moment de la brèche

-Mesures adoptées après l’incident

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Propositions d'actionnaires

Bureau du surintendant des institutions financières Canada | Office of the Superintendent of Financial Institutions Canada

NOTE D'INFORMATION

Date : Le 28 octobre 2013

Destinataires : Institutions financières fédérales

CADRE DE SURVEILLANCE DES INSTITUTIONS FINANCIÈRES

Objet : Conseils sur l'autoévaluation en matière de cybersécurité

CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Avis 11-326 du personnel des ACVM
Cybersécurité

Energy—IT Security for Industrial Control Systems in Alberta's Electrical Industry

CSA/ACVM Canadian Securities Administrators | Autorités canadiennes en valeurs mobilières

Avis 11-326 du personnel des ACVM
Cybersécurité

Les émetteurs, les personnes inscrites et les entités réglementées n'ayant pas encore évalué les risques liés à la cybercriminalité devraient tenter de trouver la meilleure façon de les gérer, notamment par les mesures suivantes :

- **sensibiliser le personnel à l'importance de la sécurité de l'information de la société et des clients et de la sécurité informatique, et au rôle qu'il a à jouer à cet égard;**

- **suivre les indications et les meilleures pratiques des associations professionnelles et des organismes reconnus en sécurité informatique;**

- **s'il y a lieu, procéder régulièrement à des tests et des évaluations de la vulnérabilité et de la sécurité chez les tiers.**

To do list - En bref

Inventaire et classification des actifs informationnels

Analyse de risque et vulnérabilités

Gouvernance - responsabilité

Procédures et mesures de sécurité

Encadrement de l’approvisionnement et des fournisseurs

Notification et gestion des incidents

Assurance

Formation , sensibilisation

COUVERTURES MULTIPLES

Les réclamations de tiers reliées à des intrusions dans nos systèmes informatiques, incluant les réclamations liées au défaut de protéger la confidentialité des données (pour autant que cela ne fasse pas déjà partie de notre police responsabilité);

Les coûts reliés à la gestion de crise (professionnels de l'informatique, recouvrement de données, relations publiques, suivi de crédit des clients affectés, etc…);

Coût associés à une demande de rançon par un pirate;

Pertes de revenus en raison de l'interruption d'accès aux systèmes informatiques;

Acteurs

pays /nations – crime organisé – hacktivistes – insiders

ACTIFS INFORMATIONNELS

- renseignements personnels
- propriété intellectuelle
- Commerciales (clients-fournisseurs-partenaires – stratégie)
- données opérationnelles

VULNÉRABILITÉS

- personnes
- processus
- technologies

OBLIGATIONS

PRÉSERVER

- Confidentialité
- Intégrité
- Accessibilité/disponibilité

RISQUES

Perte/vol

Altération/ destruction

copie

accès

Divulgation

poursuites

Diffusion

Interruption des affaires

Perte de marché

Sanctions

Responsables – personnes impliqués

C.A. – Dirigeants – IT – Legal – RH – Fournisseurs


Preuve Préparation au litige
information
Co-Contractants
Fournisseur
Cyber-Assurance
Informations
Infonuagique
Vie privée
Hacking Social
Actionnaires
Employés
financière
Régulateurs
Intrusion
Phishing
Relève
Internet des objets
industriels
Cyber-Espionnage
privilégiées
Délits d'initiés
Sous-traitant
CCQ
LCCJTI
Dénonciation de risque
Mobilité
Destruction
Obligation de notification
Secrets
Fiabilité
Conformité
Renseignements personnels
Continuité des affaires
Divulgation de risques

LANGLOIS

AVOCATS - LAWYERS

Jean-François De Rico

jean-francois.derico@langlois.ca

514-842-9512 /418-650-7923

www.langlois.ca

www.linkedin.com/in/jfderico