

Data Breach Class Actions

Presented at Aon Risk Solution's Privacy Speaker Series
October 15, 2014

Kristin Ali
416-863-2678
kristin.ali@blakes.com

The logo for the law firm Blakes, written in a cursive script.

Introduction

- Surge in data breaches has resulted in extensive civil litigation and regulatory activity in Canada and the US
- Class action plaintiffs are advancing a laundry list of claims, including the fairly new tort of intrusion upon seclusion

The logo for the law firm Blakes, written in a cursive script.

2014 Data Breaches

- Large retailers:
 - 56 million cards
 - 40 million cards + 70 million customers
- Financial institution:
 - 76 million households + 7 million businesses
- Online retailer:
 - 145 million customers
- Canadian Healthcare Provider:
 - 14,450 patients

Blakes

2014 Data Breaches (cont'd)

- Across industries
- Different types of data
- Different types of breaches
- Class actions typically follow a breach

Blakes

Data Breach Claims

- Claims Made In Recent Class Actions:
 - Negligence
 - Negligent misrepresentation
 - Breach of contract
 - Breach of fiduciary duty
 - Breach of confidence
 - Intrusion on seclusion

Blakes

Tort of Intrusion Upon Seclusion

- Created in *Jones v Tsige* in 2012 with a 3-part test:
 1. Defendant's conduct be intentional or reckless
 2. Defendant invaded the plaintiff's private affairs or concerns without lawful justification
 3. Reasonable person would regard the invasion as highly offensive, causing distress, humiliation, or anguish
- No need for economic harm or dissemination
- Courts expanded on *Jones* in 3 class action cases:
Hopkins, Condon and Evans

Blakes

Hopkins v Kay

(Jan 2014)

- 280 medical records alleged to have been accessed by employees and disseminated to third parties
- Court refused to strike the claim for intrusion upon seclusion, rejecting the hospital's argument that the compensation scheme under the PHIPA excludes common law remedies
- Not yet certified. ON CA to hear appeal on motion to strike on December 15, 2014

Blakes

Rouge Valley Health System

(No decision yet)

- Two employees alleged to have turned over personal data of 14,450 patients to companies selling RESPs
- TPS, OIPC and OSC are all investigating
- Plaintiffs seeking \$400M+ in compensation:
 - \$332M in general damages for breach of contract, breach of warranty, breach of confidence, intrusion upon seclusion, negligence, and conspiracy;
 - \$80M in exemplary or punitive damages;
 - Special damages of an undetermined amount
- Not yet certified. Waiting for outcome in *Hopkins*

Blakes

Condon v Canada

(March 2014)

- Federal government lost a hard drive containing personal info of 583,000 participants in a Student Loan program. No evidence of tangible loss
- Breach of contract and warranty (loan application forms contained terms as to how PI would be stored, disclosed and destroyed)
- Unlike *Jones*, in *Condon*, there was no intrusion, but the FC said that the ONCA had confirmed the intrusion on seclusion tort “as a category of broader tort relating to invasion of privacy”
- Class action certified

Blakes

Tort of Intrusion Upon Seclusion

- To date, no decision considering new tort on the merits in data breach context
- Concern that tort is being used more broadly by plaintiffs than ONCA intended
- BUT difficult to prove conduct was intentional or reckless and highly offensive for data breaches
- Damages capped at \$20,000, punitive damages only in “truly exceptional” cases

Blakes

Legal Costs of Data Breach

- Legal costs vary depending on the size of the breach, the nature of the information stolen, and the extent of litigation and regulatory activity
- In 2013, average cost to a company was US\$3.5 million and 15% more than what it cost the previous year
 - Ponemon Inst., 2014 Cost of Data Breach Study: Global Analysis
- Reports of Target incurring \$148 million to date in direct expenses related to its data security breach but partially offset by \$38 million in insurance

Blakes