

Cross Border Data Breach Response



**LITIGATION
CONFERENCES**

Speakers



Ted Augustinos, *moderator*
Partner
Locke Lord

James Creasy
Class Underwriter
Novae



Alex Cameron Fasken
Partner
Fasken Martineau

Shannon Groeber
Senior Vice President
JLT

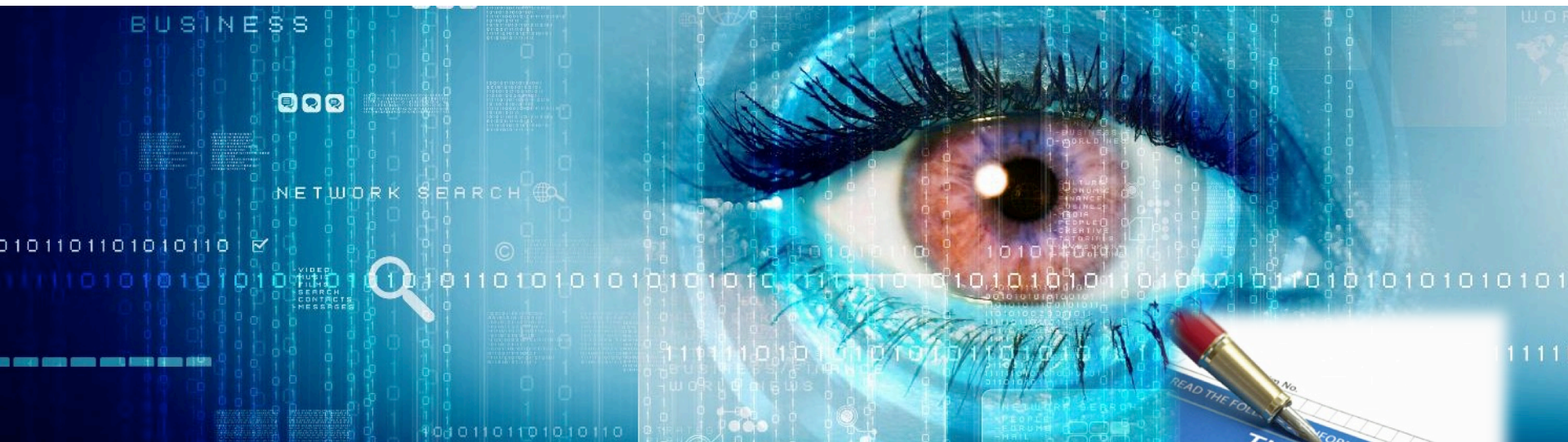


Bo Holland
CEO
AllClear ID

Dr. Thomas Rothärmel
Munich Re



EU General Data Protection Regulation (GDPR) Implications



Highlights

NetDiligence®

I. Objective:

Update and harmonise EU data protection law
(now: 28 different laws and 28 independent data protection authorities)



**LITIGATION
CONFERENCES**

II. Territorial scope:

1. Activities of an establishment of a controller or a processor in EU,
2. If controller or processor does not reside in EU, if processing is related to:
 - offering of goods or services to subjects in EU (new! = expanded scope of application)
 - monitoring of behavior of subjects, limited to behavior in EU



III. Applicable 26 May 2018



III. For the first time in all EU member states: Notification obligations in case of personal data breaches

- Compulsory notification of **data protection authorities** in case of data breaches
- Compulsory notification of **victims**: Only if data breach is “likely” to result in a “high risk” to rights and freedoms of natural persons
- A number of exemptions (e.g. “when disproportionate effort required”)



Highlights

NetDiligence®

IV. New obligations for Data Controllers and Processors

V. Drastic fines in case of infringements of up to 4% of global annual turnover

VI. Right to compensation and damages broadened



**LITIGATION
CONFERENCES**

Canada: Key Developments

- New breach notification provisions
- Unprecedented litigation activity
- Emerging regulatory guidance
- Cross border response issues

New breach notification provisions

- **Notice to:** Commissioner, individuals & others
- **Threshold:** “real risk of significant harm”
- **Form:** direct notice is default
- **Timing:** “as soon as feasible”

New breach notification provisions

- Notice must contain sufficient information:
 - to allow an individual to understand the **significance** of the breach to them, and
 - to take steps, if possible, to **reduce the risk** of harm or **mitigate** it, and
 - any other prescribed information

New breach notification provisions

- Record keeping:
 - Organizations must keep a record of **every breach**
 - Commissioner may obtain all breach records
- Information sharing/publication
- Offences and fines up to \$100,000

Unprecedented litigation activity

Highlights of Privacy Litigation and Damage Awards in Canada 2010-2016

Alan Cameron, Fasken Martineau

Case	Allegations	Claims	Status
<i>McPhy v. Bellco, 2013 BC 570</i>	Disclosure of private communications to other staff in the public.	Defamation and breach of statutory privacy law.	\$40,000 for breach of privacy and defamation.
<i>Lafuze v. National Bank, 2015 QC 592</i>	Leaking stolen, 225,000 affected. Actual fraud and ID theft.	Negligence in submissions, failure to alert credit monitoring, false, failure to notify.	Class certified. Court approved settlement on August 1, 2015.
<i>Randall v. Madonna, 2010 FC 159</i>	Firm used disclosed number of visits to the complainant's employer.	Breach of PIPEDA.	No damages. Breach was the result of a procedural error.
<i>Nimmo v. Translink, 2015 FC 199</i>	Could have been disclosed escalate credit report to bank for loan application.	Breach of PIPEDA.	\$5,000 in damages, including apology and lettering.
<i>ACTE v. Phoenix, 2015 BC 592</i>	Attachment of doctor's report to original medical file of case filed by the plaintiff.	Claim for breach of contract, breach of statutory privacy law, and invasion of privacy.	Privacy claim dismissed. Absolute immunity for court proceedings.
<i>Lind v. Laker, 2011 MB 26</i>	Use of dates of patients without consent, and refusal to return documents.	Violation of privacy. Quantum of damages adjusted to trial.	\$100,000 in damages.
<i>Gray v. Avon, 2005 FCT 607</i>	Sales rep published a list report from the DPI, in a PIPEDA complaint.	Breach of PIPEDA.	\$1,500 award. Dependent damages but no tort award.
<i>Landy v. Royal Bank of Canada, 2011 FC 887</i>	Disclosure of information to complainant's ex-spouse in divorce proceeding.	Breach of PIPEDA.	\$4,500 in damages, considering contributory fault and humiliation.
<i>St-Ange v. Desjardins, 2015 FC 139</i>	Flawed/changed privacy settings. Confidential information revealed public.	Unjust enrichment, invasion of privacy, breach of confidence.	Court decided administrative forum does not have jurisdiction to hear damages before \$10,000 and interest.
<i>Landy v. Bank of Montreal, 2011 FC 887</i>	Defendant used Open Peer Inspection (OPI) to inspect internet traffic.	Defamatory remark. \$2,000 in damages. Also for invasion of privacy. OPI was to manage traffic, not inspect.	Class certified. No reported decision or settlement.
<i>Alshay v. Google, 2011 FC 109</i>	Unauthorized data collection from e-mails by Google through data.	Violation of privacy rights. Remediation.	No reported decision or settlement.
<i>Smith v. Honda, 2011 ON SC No. 7308/11</i>	Inadequate safeguards to protect customer information in database.	\$200 million class action. Breach of privacy.	No reported decision or settlement.

Case	Allegations	Claims	Status
<i>IBRC v. AUSA, 2014 OCA 1461, 2014 OCA 1462</i>	Last unauthorised laptop with information of 52 employees.	Class action for \$1,000 per individual. Court decided in equity class due to lack of harm. Public Access above.	Pending.
<i>PJ Chirba Public Service Employees Union (Canada) v. Chirba, 2014 FC 1942</i>	Employer accessed an individual's employment insurance information without authorization.	Grievance based primarily on Jones v. Pugh contract law privacy tort.	Grievance dismissed and no damages awarded. Courts not accordably liable for actions of rogue employee.
<i>Gray v. Desjardins, 2015 FC 199</i>	Plaintiff's personal injury litigation commenced action against defence company relating to evidence.	Violation of statute, invasion upon autonomy, negligence and violation of privacy (PIPA and PIPEDA).	Claims dismissed on a motion for summary judgment, upheld on appeal.
<i>Compton v. Canada, 2015 FC 154, 2015 FC 156</i>	Class (100 and over affected) 100,000 individuals (PIA name, SIN, OCR, address and student card details).	Class action certified. See also <i>CF v. Canada</i> , 2015 FC 156.	\$200 million class action.
<i>Zimmerman v. Tseax, 2015 OCA 582, 2015 OCA 583, 2015 OCA 584</i>	Hack. Payment card and other information about 780,000 Canadians.	Negligence.	Certification pending.
<i>Heintz v. Koh, 2014 ONCJ 121, 2015 ONCJ 112</i>	Access and dissemination of medical records affecting 200 patients.	Invasion upon seclusion. Proposed class action.	ONCA has ruled that tort claims are available against organizations regulated by PIPEDA. Lapses to SCC dismissed.
<i>Ali v. KFC, 2013 BC 592</i>	Unauthorized access to information by employees of KFC.	Proposed class action. Application to certify class.	Claims in warranty liability against KFCBC were struck.
<i>Bremer v. 2000 Finance, 2015 QC 318</i>	Last date type. Actual fraud and ID theft alleged.	Negligence leading to breach and negligence in response.	Class action certified. Informalized version of <i>Madonna's</i> same incident.
<i>LaRose v. Air Canada, 2015 FC 199</i>	Hacking affecting an estimated 56 million records, including in Canada.	\$300 million proposed class action.	Pending.
<i>Alshay v. Bank of Montreal, 2013 FC 887</i>	Unauthorized change of address not timely corrected. No harm suffered.	Breach of FC Private Act negligence. Breach of contract privacy policy.	Negligence dismissed. \$2000 awarded for breach of privacy and contract.
<i>See also Cameron v. 2014 ONCJ 209</i>	Unauthorised access to information for profiling and advertising purposes.	\$750 million. Contract. Statute. Invasion upon seclusion. Involvement of tort.	Pending. See also <i>TD Bank Report of Privacy 2013</i> .

¹ But see *Langer v. FIBC pending*
² See also *Cameron v. 2014 ONCJ 209* and *Langer v. Luster, 2014 ONCJ 226* at par. 47-50.

Case	Allegations	Claims	Status
<i>Alshay v. Bank of Montreal, 2013 FC 887</i>	Last date type. Information about 53,000 employees who received H1N1 vaccine.	Sufficiency. Negligence. Invasion upon seclusion. Privacy. PIPEDA, and Charter.	Class certified. Defined as \$100,000 of damage, and by reference to show harm.
<i>Pharmco v. Pharm, 2011 BC 29</i>	Access to retirement files, documents and statements and access to health care.	Statutory privacy law, and "openness, subject and respect to privacy."	\$50 and \$300 nominal damages for breach of privacy.
<i>Pharmco v. Columbia, 2012 BC 390</i>	Unlawfully disclosure of mental records and providing medical records.	Negligence, fraud, and breach of Privacy Act.	No privacy in documents relevant to litigation. Injunction not granted.
<i>Pharmco v. Columbia, 2012 BC 390</i>	Class. Document that partly information in divorce proceeding.	Breach of PIPEDA.	\$3,500 award. Plaintiff objected to the disclosure and sufficient mitigation.
<i>Donovan v. BC Health Services, 2015 FC 156</i>	Medical records not reviewed adequately and not returned to the plaintiff.	Breach of PIPEDA.	No damages. Policies and procedures were in place. An error and delay were not caused.
<i>Mackinnon v. University of Regina, 2014 FC 259</i>	Last date type in typed with name, address, phone, OCR, credit information, and SIN.	Negligence. Storage, security, invasion, failing to follow protocol.	Defendant denied. No composite damage found only a list of CFI's.
<i>John v. Sage, 2013 OCA 24</i>	Bank employee accessed customer information over text and printed.	Invasion upon seclusion and breach of statutory law.	\$10,000 for invasion upon seclusion. Contract dismissed and agency made.
<i>John v. Sage, 2013 OCA 24</i>	Employee's accessed patient personal information and health information for non-work related purposes.	Proposed class action for invasion upon seclusion, negligence, invasion of privacy, breach of contract.	No reported decision or settlement.
<i>John v. Sage, 2013 OCA 24</i>	Unauthorized access to electronic files of employees in Progress of their employment in the course of a plaintiff proceeding.	Breach of the Freedom of Information Act and breach of Privacy Act. Tort of invasion and the Charter.	\$1,250 to each of 25 employees. Breach of contract. Breach of contract. Breach of contract. Breach of contract.
<i>John v. Sage, 2013 OCA 24</i>	Collection and use of information in Great messages for ads.	Breach of Privacy Act. Confession. Common law privacy. Competition Act.	Pending.

¹ See also *Charney v. Greater Regional Health, Newfoundland Superior Court, No. 2012 2012 FC 129*. See *Yip v. Western Regional Health, Newfoundland Superior Court, No. 2012 2012 FC 129*.

Case	Allegations	Claims	Status
<i>Cartwright v. 2013 BC 592</i>	Inspection of property, including residences and vehicles rendered.	Application to dismiss action by defendants for invasion of privacy.	Inspection authorized by law. No privacy tort.
<i>Active Auto Leasing v. 2015 QC 189</i>	Defendant's mother received occasional calls by defendant's wife in banking and the dollar amount using.	Disclosure of private facts.	\$100 for privacy tort as a set-off. All five party torts recognized.
<i>Luce v. Procter & Gamble, 2015 FC 320</i>	Hacking incident of online banking file affecting about 12,000 accounts.	Proposed class action seeking \$13 million.	Certification pending. See also <i>TEICOA Report of Privacy 2015</i> .
<i>Grant v. Absorb, 2013</i>	Low USD affecting 25,000 patients.	Proposed class action seeking \$4 million.	No reported decision or settlement.
<i>See also, The Queen, Fed. Ct. 1391, 13, 2013 FC 138</i>	Letters to individuals with "National Medical Access Program" on envelope.	Class action certified. See also <i>Fédération de la Santé de la Province (FCSP) v. Health Information Commission Report of Privacy Act, breach of privacy, contract, negligence, etc.</i>	Class action certified. See also <i>Fédération de la Santé de la Province (FCSP) v. Health Information Commission Report of Privacy Act, breach of privacy, contract, negligence, etc.</i>
<i>Abdi v. Apple Inc., 2015 OCA 295</i>	Class action against Apple for collecting and sharing information without consent.	Breach of privacy, contract and misrepresentation.	Class action certified.
<i>Conkover v. Bell, 2013 FC 138</i>	Unauthorized credit check. Claimant requires impact on credit rating.	Breach of PIPEDA.	\$15,000 damages, \$15,000 exemplary damages, \$10,000 costs.
<i>Abu-Adwan v. Ford, 2015 FC 156</i>	Ford accessed 10,000 employees' information to an unsecured website.	\$14 million proposed class action for risk of ID theft. Cost of prevention, mental distress.	Pending.
<i>Milnes v. St. John's, 2015 FC 156</i>	Sony localization network hack. Unauthorized access to electronic messages potentially affecting 77 million.	\$1 billion class action.	Settlement proposed for various benefits, depending in part on an individual's account type.
<i>Doyle v. Anderson, 2014 BC 262</i>	A physician attempted to obtain a hospital personal information about another physician to discredit him.	Defamation, tort, slander, invasion of privacy, breach of contract, negligence, tort, invasion of privacy, breach of statutory privacy law.	\$100,000 general damages, \$10,000 aggravated damages, for defamation and privacy tort for malicious purpose.
<i>Edmonton (City) Police v. Edmonton (Town Assn.), 2015 OCA 464, 465</i>	At a staff meeting, inappropriate suggestions were made regarding the groom's health and emotional condition.	Invasion of privacy.	\$3,000 awarded. Police vulnerable to harm with peers arising from disclosure of alleged mental health condition.

Case	Allegations	Claims	Status
<i>Shah v. Petro-Canada Regional Health Authority, 2013 FC 447</i>	Defendant disclosed information to the plaintiff who died in an emergency room without treatment.	\$10,000 for the privacy claim. Statutory privacy tort as <i>Morisy</i> , negligent disclosure of personal information.	Order striking the claim as set aside. Whether the claim discloses causes of action is referred to a new judge.
<i>Horsell v. South Hill, 2015 FC 156</i>	Fraudulent misrepresentation of medical records in an unauthorized manner.	Invasion upon seclusion and vicarious liability.	Class action certified. Common issues trial April 2016.
<i>Morris v. Sun Life of Canada, 2013 FC 138</i>	Sixto searches of 10 financial privacy records.	Invasion upon seclusion and breach of the Charter.	Class action certified.
<i>Eidson v. BMO v. 2015 FC 156</i>	Unauthorized access and disclosure of sensitive information by employer.	\$3 million proposed class action. Invasion upon seclusion. Vicarious liability. Section of tort.	Proposed class action.
<i>Do v. MTS, 2015 FC 156</i>	Plaintiff was wrongly posted an extensive record of their use of internet services without knowledge or consent.	Breach of confidence, intentional infliction of mental distress, invasion of privacy (specific disclosure of private facts).	\$147,100.00 awarded, with litigation. Recognizes tort of public disclosure of private facts.
<i>Shah v. Anshu, 2015 FC 156</i>	Defendant misrepresentation that the web is lower and so, as well as the plaintiff's information with them, thinking the plaintiff's information was not shared.	Fraudulent misrepresentation, invasion upon seclusion.	\$5,000 awarded for invasion upon seclusion and punitive damages.
<i>M.M. v. Family Aff. (Canada), 2015 FC 156</i>	200 individuals' information relating to child and family welfare services. Confidential information, which was hacked and publicly disclosed.	\$75 million proposed class action. Negligence. Breach of contract. Breach of privacy.	Proposed class action.
<i>Dunn v. Saskatchewan (Health Services), 2015 FC 156</i>	Unauthorized laptop with 600,000 patients' information open, including names, OCR, health care numbers, and diagnostic codes.	\$11 million proposed class action.	Proposed class action. Settlement pending court approval in July 2016 for payment of \$100,000 disclosure of covered facts and other terms.



Unprecedented litigation activity

- *Lozanski v. Home Depot*, 2016 ONSC 5447:

“The case for Home Depot being culpable was **speculative** at the outset and ultimately the case was proven to be **very weak**. The real villains in the piece were the computer hackers, who stole the data. After the data breach was discovered, there was no cover up, and Home Depot responded as a good corporate citizen to remedy the data breach. ...”

Unprecedented litigation activity

- *Canada v. John Doe*, 2016 FCA 191:

“At best, the material facts pleaded support the notion that an **isolated administrative error** was made. This is a far cry from the situation in *Tsige*, where a bank employee accessed private financial information.... Here, there are no material facts pleaded to support an allegation of bad faith or recklessness.”

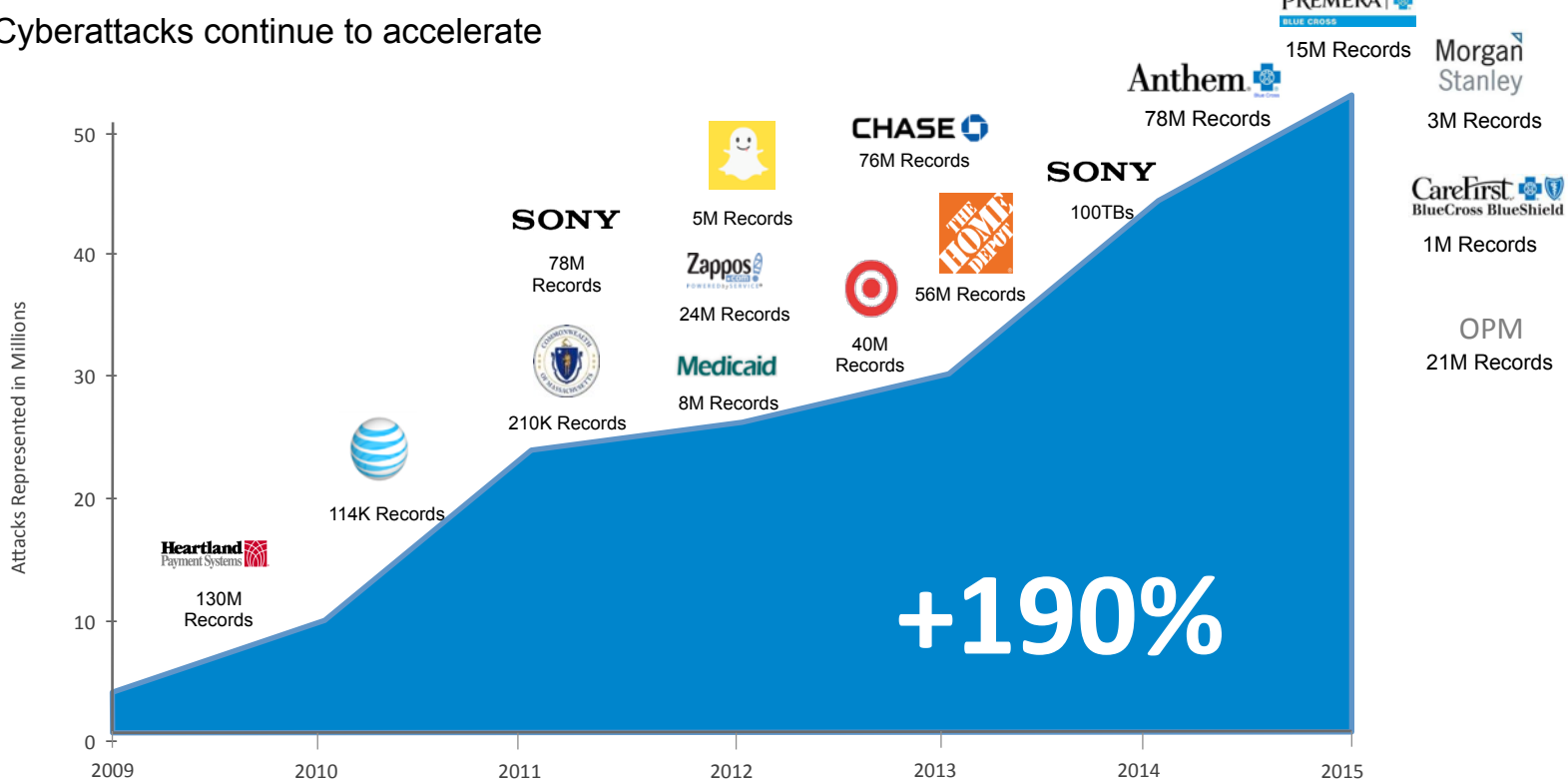
Emerging regulatory guidance

- Recent weeks/months:
 - CSA Staff Notice 11-332: Cyber Security
 - MFDA Bulletin 0690–C: Cybersecurity
 - OSFI Report on Plans and Priorities
 - IIROC cybersecurity “report cards”

Cross border response issues

- Unique notice and federal/provincial jurisdiction issues
- Cross-border transfers may be prohibited or restricted (even in an investigation/response)

- Cyberattacks continue to accelerate



Sources: 2015 PWC Global State of Information Security Survey; Identity Theft Resource Center

Proprietary & Confidential AllClear ID

17

10/18/16

Expect more like this...



“Samsung’s Exploding Note”



Scared Customers



Executive Accountability



Open House for Regulators

10/18/16

Proprietary & Confidential AllClear ID

18

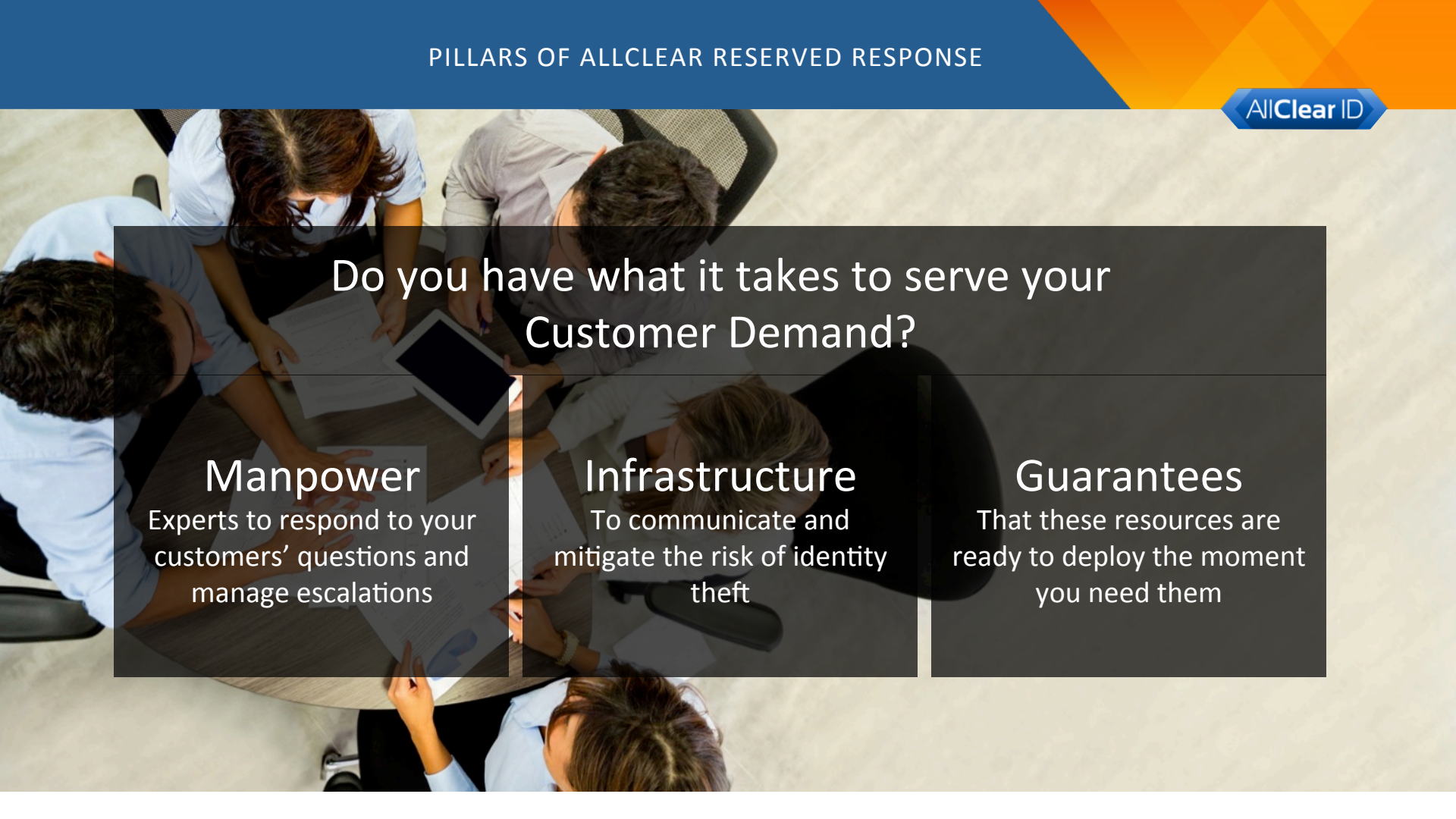
IT REQUIRES A SPECIAL OPERATIONS TEAM

	CYBER INSURANCE	ATTORNEY	FORENSICS	CUSTOMER RESPONSE
PRE-BREACH	Underwrite, Sell & Service Cyber Policy	Create Incident Response Plan	Set up the Environment & Protocols for Investigations	Forecast demand, plan the customer response, reserve the manpower & infrastructure
ACTIVE BREACH	Manage the Claim	Manage the Event & Determine if Notifiable	Investigate & Determine if there is a Breach and who was Affected	Provide Notification, Call Center & ID Protection



**LITIGATION
CONFERENCES**

NetDiligence®



Do you have what it takes to serve your Customer Demand?

Manpower

Experts to respond to your customers' questions and manage escalations

Infrastructure

To communicate and mitigate the risk of identity theft

Guarantees

That these resources are ready to deploy the moment you need them

Questions?

NetDiligence®

Ted Augustinos

ted.augustinos@lockelord.com

James Creasy

JCreasy@novae.com

Alex Cameron Fasken

acameron@fasken.com

Shannon Groeber

Shannon.Groeber@JLTUS.com

Bo Holland

bo.holland@allclearid.com

Dr. Thomas Rothärmel

TRothaermel@munichre.com

Thank you!



**LITIGATION
CONFERENCES**