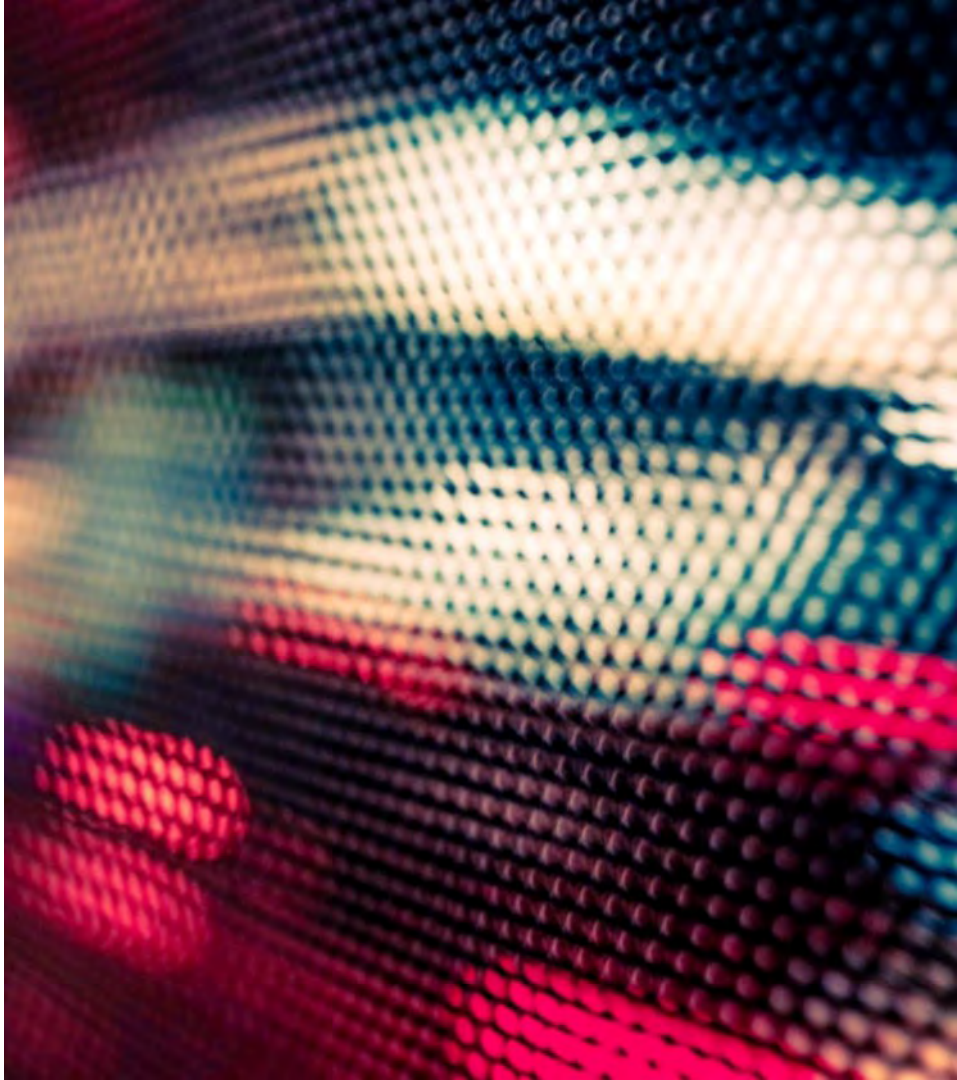
NORTON ROSE FULBRIGHT

ALIA Cyber Coverage Webinar:

Breach Response and Privacy Obligations

Alberta Lawyers Indemnity Association
June 13, 2023



Welcome message

David Weyant, K.C.
President and CEO
Alberta Lawyers Indemnity Association

ALBERTA LAWYERS
INDEMNITY ASSOCIATION

Table of Contents

- Team introduction
- Overview of the current cyber threat landscape
- Incident management and response
- Legislative overview and changes
- Key decisions
- Cyber insurance trends and examples
- Refresher of the ALIA universal cyber offering and claims response services

Team Introduction

Norton Rose Fulbright Canada LLP, Breach Coach

Imran Ahmad

Partner
Canadian Head of Technology,
Co-Head of Information
Governance, Privacy and Cybersecurity
Toronto & Montréal
Tel: +1 416 202 6708 | +1 514 847 4747
E: imran.ahmad@nortonrosefulbright.com

- Imran advises clients across all industries on a wide array of technology-related matters.
- He works very closely with clients to develop and implement practical strategies related to cyber threats and data breaches. He advises on legal risk assessments, compliance, due diligence and risk allocation advice, security, and data breach incident preparedness and response.
- Imran acts as "breach counsel" in the event of a cybersecurity incident, such as a data or privacy breach, and has extensive experience in managing complex security incidents and cross-border breaches. He also provides representation in the event of an investigation, an enforcement action or a litigation.
- Imran is the author of Canada's first legal incident preparation and response handbook.

John Cassell

Partner
Co-Head of Information
Governance, Privacy and Cybersecurity
Calgary
Tel: +1 403 268 8233 | +1 403 835 8643
E: john.cassell@nortonrosefulbright.com

- John is Co-head of Norton Rose Fulbright Canada LLP's information governance, privacy and cybersecurity team.
- John assists clients with all manner of privacy and cybersecurity law issues including: acting as breach counsel in responding to cybersecurity incidents, advising on cyber and privacy risk management strategies including pre-incident cyber-security preparedness and privacy/cyber vulnerability and gap assessments and assisting clients in responding to civil claims and regulatory investigations and enforcement actions arising out of cybersecurity incidents.

Norton Rose Fulbright Canada LLP, Breach Coach

Travis Walker

Senior Associate
Technology, Information Governance, Privacy and Cybersecurity
Toronto
Tel: +1 416 216 4819
E: travis.walker@nortonrosefulbright.com

- Travis is a senior associate practicing in the areas of information governance, privacy and cybersecurity law.
- He guides clients through each phase of the breach response and remediation, including the restoration of data systems, retention of forensic experts, notification to affected individuals and stakeholders, and reporting to regulatory authorities.
- He also consults on the development and implementation of information governance policies and procedures, including incident response plans, privacy policies and breach preparedness.

Our team

Ontario	Quebec	Alberta	British Columbia
Imran Ahmad, Partner Stephen Nattrass, Partner Travis Walker Suzie Suliman Shreya Gupta Tiana Corovic Roohie Sharma Katarina Duke Marisa Kwan	Imran Ahmad, Partner Veronique Barry, Partner Kasandra-Rose Villeneuve Katherine Barbacki Roxanne Caron Jérémie Wyatt Stephanie Fontana	John Cassell, Partner Ann Henderson Erin Colwell	Alexis Kerr, Partner Sara Levine, Of Counsel

Overview of the Current Cyber Threat Landscape

Overview of the Current Cyber Threat Landscape

- **According to the World Economic Forum's Global Risks Report 2023**, widespread cybercrime and cyber insecurity is among the top 10 risks identified by companies that they could face over a 2-year and 10-year period.
- **Impact on:**
  - Operations
  - Reputation (media, shareholders, business partners, employees)
  - Financial losses due to operational disruption and litigation (Statista → $5.64 million USD in 2022)
  - Legal & Regulatory

- **Boards and SLTs are focused on resiliency,** which is the means by which a victim organization bounces back from a cybersecurity incident
- **Numerous cyber threats but key ones to focus on:**
  - Ransomware
  - Third-party breaches
  - Business email compromise (also known as BECs)

Overview of the Current Cyber Threat Landscape

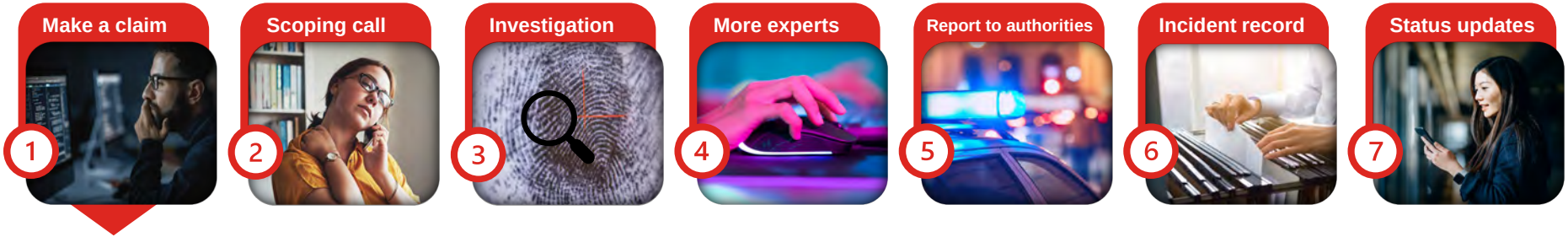
- **According to IBM's Cost of a Data Breach Report,** the global average cost of recovery from a ransomware incident is $4.54 million USD.
  - Ransomware accounted for 11% of the types of breaches experienced by organizations in 2022.
- **In 2021, more than half of all Canadian ransomware victims were in the critical infrastructure sector,** such as health, energy, and manufacturing.
  - The critical infrastructure sector remains a prime target for cybercriminals and state-sponsored actors.

- **Since January 2020, attackers are employing dual and even triple extortion techniques:**
  - Data encryption ► operational disruption
  - Data theft ► sensitive data
  - Escalation tactics ► reputational harm
- **Quantum of ransom demands has materially gone up** (often between $2-10 million)
- **Challenge assessing value of data**
  - Personal information / personal health information
  - Sensitive corporate data
  - Sensitive third-party data
  - Cyber insurance considerations

NRF

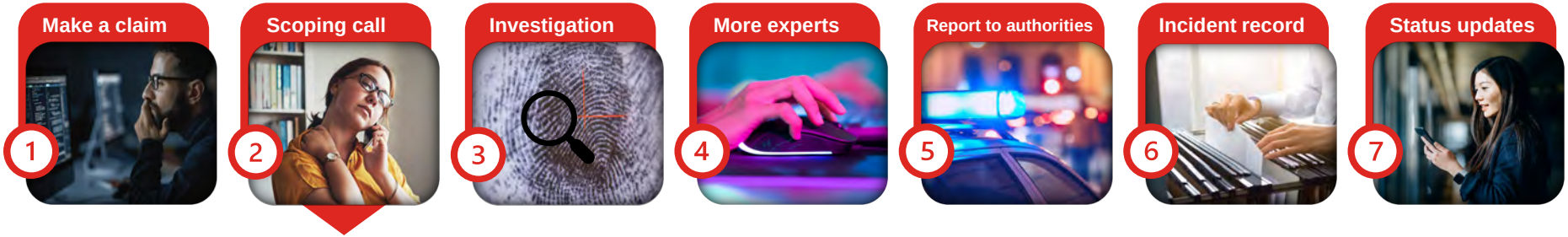
Incident Management & Response

You've been breached, now what?



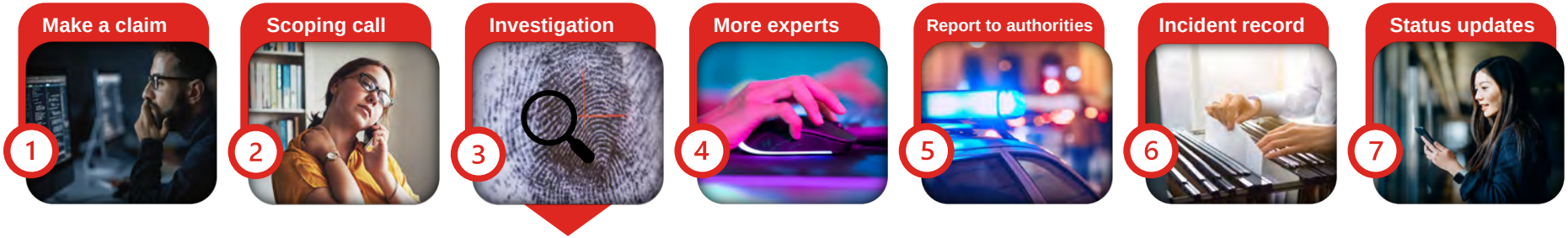
Victim organization experiences a cybersecurity incident and initiates a claim.

You've been breached, now what?



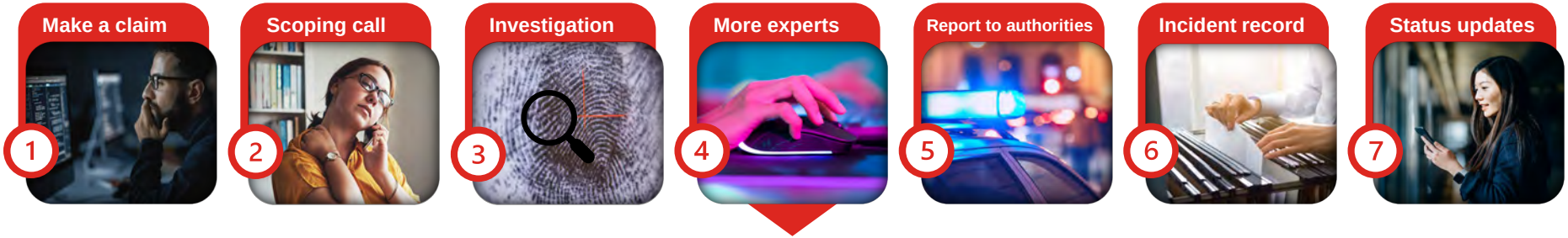
NRF is notified and schedules a scoping call with the Insured the same day.

You've been breached, now what?



As Breach Coach, NRF retains forensic firms on behalf of the Insured to assist with containment, remediation and to conduct a forensic investigation into the cause and scope of the Incident.

You've been breached, now what?



If required, NRF may also retain service providers to:

- negotiate with the Threat Actor (in the case of ransomware) to gain intelligence and/or potentially make a ransom payment;
- conduct data mining to determine whether sensitive or personal information was impacted; and/or
- obtain credit monitoring solutions, assist with notifying affected individuals and potentially establish a call centre for affected individuals

You've been breached, now what?

1. Make a claim

2. Scoping call

3. Investigation

4. More experts

5. Report to authorities

6. Incident record

7. Status updates


Report the incident to law enforcement and regulatory authorities.

You've been breached, now what?

1. Make a claim

2. Scoping call

3. Investigation

4. More experts

5. Report to authorities

6. Incident record

Prepare an overview of the incident for the Insured's records.

7. Status updates

You've been breached, now what?

1. Make a claim

2. Scoping call

3. Investigation

4. More experts

5. Report to authorities

6. Incident record

7. Status updates


Throughout this process, NRF provides regular status updates to the assigned adjuster regarding outlook, risk and anticipated expenses.

You've been breached - process summary

- Victim organization experiences a cybersecurity incident and initiates a claim.
- NRF is notified and schedules a scoping call with the Insured the same day.
- As Breach Coach, NRF retains forensic firms on behalf of the Insured to assist with containment, remediation and to conduct a forensic investigation into the cause and scope of the Incident.
- If required, NRF may also retain service providers to:
  - negotiate with the Threat Actor (in the case of ransomware) to gain intelligence and/or potentially make a ransom payment;
  - conduct data mining to determine whether sensitive or personal information was impacted; and/or
  - obtain credit monitoring solutions, assist with notifying affected individuals and potentially establish a call centre for affected individuals
- Report the incident to law enforcement and regulatory authorities.
- Prepare an overview of the incident for the Insured's records.
- Throughout this process, NRF provides regular status updates to the assigned adjuster regarding outlook, risk and anticipated expenses.

Common Cyber-Incidents & Attack Vectors

- Malicious software – refers to any program or codes that is created with the intent to do harm to a computer, network of server
  - e.g., ransomware, Trojan, exploits

- Uses email, SMS, phone, social media and social engineering techniques to entice a victim to share sensitive information such as login credentials or to download a malicious file

- Technique whereby the threat Actor disguises themselves as a known or trusted source to gain information, install malware, extort money
  - e.g., email spoofing, domain spoofing

Common Cyber-Incidents & Attack Vectors

Password exposure or theft

- Gaining access to a system through valid credentials
  - Difficult to detect as a threat actor may act as the legitimate user
  - e.g., pass-the-hash, credential stuffing, password spraying

System vulnerabilities

- When vulnerabilities in a software or application are not yet rectified by a software update or patch these vulnerabilities can be exploited by threat actors
  - e.g., Log4j, ZeroLogon

Infected storage media

- Discs, memory sticks and USB drives containing malicious software

Ransomware Incidents – Should you Pay?

- **Factors to consider**
  - Availability of backups
  - Ability to rebuild from scratch
  - Whether data has been exfiltrated
  - Amount of the ransom

- **Risks**
  - No guarantee that threat actor will provide decryption tool once payment is made
  - No guarantee that the decryption tool will work
  - Potential re-extortion demand after initial payment

- **Other considerations**
  - Paying could encourage further attacks and result in regulatory action if payment made to government-sanctioned groups or individuals. Sanction laws clearance must be obtained prior to potential payment.

Managing Third Party Data Breaches

Third party data breaches may force you to respond to cyber incidents occurring outside of your organization.

- When responding to a third party data breach, consider:
  - Have you received sufficient information from the third party to assess the scope and extent of the incident? (date of incident, data impacted etc.)
  - What are your contractual obligations with the third party?
  - Who has control over the data?
  - Who is required to notify affected individuals?
  - Who is reporting this incident to regulatory authorities?
  - What is the communication strategy to media and stakeholders?

Communication is key to effectively managing a third party breach, especially in the event the breach is made public. A clear communications plan between the organization experiencing the breach and the organization(s) whose data may have been compromised can go a long way in mitigating the impact.

Post-Breach Remediation

- **Lessons learned**
  - The Incident Response Team (with legal counsel) to discuss what worked well and what didn't and build on any lessons learned, including security gaps identified during the forensic investigation.

- **Cyber Incident Response Plan (CIRP)**
  - Develop or update a CIRP
  - CIRP should outline specific steps to be taken when responding to cybersecurity incidents including pre-onboarding incident response vendors

- **Data Retention Policy**
  - Develop or update data retention policy

- **Cybersecurity Awareness Training**
  - Implement cybersecurity user awareness program and conduct regular training

- **Third-party due diligence**
  - Implement or update cybersecurity provisions in all contracts with third parties who process personal information and introduce cybersecurity provisions where appropriate

Regulatory Requirements - Overview & Anticipated Changes

Alberta's *Personal Information Protection Act* (PIPA)

- PIPA is Alberta's private-sector privacy legislation and applies to private-sector organizations doing business in Alberta and the collection, use and disclosure of personal information.

- Under PIPA, it is mandatory for an organization with personal information under its control to notify the Office of the Alberta Information and Privacy Commissioner (OIPC), without unreasonable delay where:

a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, unauthorized access to or disclosure of personal information.

- The OIPC has the power to require an organization to notify affected individuals when a privacy breach presents a real risk of significant harm to individuals as a result of the breach.

- Non-compliance with PIPA may result in fines, an investigation and/or an investigation.

- Once reported, if the OIPC is in agreement that the mandatory breach reporting test has been satisfied, it will subsequently publish a breach reporting decision on its website.

- British Columbia's *Personal Information Protection Act* effectively mirrors Alberta's PIPA with the exception that it does not contain mandatory breach reporting obligations.

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Applies to private-sector organizations across Canada that collect, use and disclose personal information in the course of commercial activities and includes federally regulated organizations that conduct business in Canada.
- Applies to cross-border transfers of personal information and the collection, use and/or disclosure of personal information of individuals in Provinces that have not enacted provincial privacy legislation (outside Alberta, B.C. Quebec).
- Personal information means information about an identifiable individual.
- An organization is required to notify affected individuals and report an incident to the Privacy Commissioner where there is a breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual .
- Significant harm covers a wide range of situations including bodily harm, embarrassment, financial loss, fraud, identity theft.
- Non-compliance with PIPEDA may result in an investigation, audit and/or fines.

Meaning of “control”

- “control” is not defined in either PIPEDA or PIPA.
- PIPEDA’s accountability principle provides that an organization remains responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.
- Alberta’s Privacy Commissioner has provided guidance that information is under the control of an organization when the organization “has the authority to manage the information, including restricting, regulating and administering its use, retention and disposition, and demanding the return of the information.”
- When dealing with third party service providers, we recommend clearly establishing which entity has control over the information.

Law 25 – Quebec

Quebec's Bill 64 adopted in September 2021. Law 25 came into force in September 2022

- Mandatory notification and incident record-keeping obligations took effect in 2022.
- Where a person carrying on an enterprise has cause to believe that a confidentiality incident involving personal information the persons holds presents a serious risk of injury to affected individuals, the person carrying on an enterprise must promptly notify the Commission d'accès à l'information. Affected individuals must also be notified.
- New obligations coming in 2024

- September 2023
  - Develop and publish data protection and confidentiality policies
  - Assessments for transfer of personal information outside of Quebec
  - Mandatory provisions within outsourcing contracts
  - Increased penalties and fines – up to $25,000,000 or 4% of worldwide revenue

- September 2024
  - Data portability rights

Bill C-27: Digital Charter Implementation Act

Part 1: Consumer Privacy Protection Act enactment

- Repeals Part 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)
- Reforms Canadian privacy laws and promotes electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities
- Includes a number of changes that were introduced in Bill C-11

Part 2: *Personal Information and Data Protection Tribunal Act* enactment

- Establishes an administrative tribunal
- Imposes penalties for contravening provisions in the Act

Part 3: *Artificial Intelligence and Data Act* enactment

- Regulates international and interprovincial trade and commerce in artificial intelligence systems

Key Decisions – Breach Response

Key decisions – Breach Response

***Chow v. Facebook*, 2022 BCSC 137**

- Plaintiffs sought to certify a class action for breach of privacy (statutory tort), unjust enrichment and unlawful means on the basis that Facebook extracted call and text data from users of its Android Messenger app without their knowledge or consent
- Certification denied; Plaintiffs failed to show some or any basis in fact for central allegation that Facebook misused call and text data to enrich itself
- Certification remains a low hurdle but a hurdle nonetheless; Court has an important gatekeeping function to weed out claims of dubious merit early in the certification process (*Kish*, 2021 SKQB 198; *Simpson*, 2021 ONSC 968)

Key decisions – Breach Response

RE: Capital One Consumer Data Security Breach Litigation, MDL No. 1:19md2915 (AJT/JFA)

- In determining whether a document was created in anticipation of litigation, a court must determine whether the driving force behind the preparation of requested document was for litigation or business.
- Here, the Court found that the forensic report was prepared for business purposes as Capital One had contracted with the forensic firm to provide this information prior to having legal counsel involved.

Lévy c. Nissan Canada Inc., 2019 QCCS 3957 & 2021 QCCA 682

- Nissan experienced a ransomware event in December 2017 and notified affected Canadians of the incident in January 2018.
- The Court noted that under PIPEDA, notice shall be given as soon as feasible after the organization has determined that the breach has occurred, “reflecting that care is required to reduce the period of time during which personal information may be used by others before the persons concerns know and can try to protect themselves adequately.” at paras 78-79

ALIA Universal Cyber Insurance Program

ALIA Universal Cyber Program Overview

Liability Claim Costs

	Deductible
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 1. Security Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 2. Privacy Liability Coverage**	$5,000
$250,000 each Claim / $250,000 Aggregate each Law Firm **For Coverage 4. Regulatory Proceedings**	$5,000

35

ALIA Universal Cyber Program Overview

First Party Response Costs

	Deductible
$35,000 each Claim / $35,000 Aggregate each Law Firm **For Coverage B Breach Cost coverages, Cyber Extortion Coverage**	$5,000

Maximum amount claimable per firm in a policy period is $285,000

How to Report a Claim

Urgent crisis management and/or reporting of a claim/ circumstance

If urgent crisis management or legal advice is needed following a cyber attack: Please contact the designated incident response breach coach: **Designated Breach coach** **Imran Ahmad** 1-866 -BREACHX / 1-866-273-2249 nrfc.breach@nortonrosefulbright.com This contact information is toll-free and available to access 24 hours 7 days a week.	To provide formal notice of a claim or a circumstance to the insurer: Send claim details to: **Notification Email**: Claims@zurich.com Phone: 1-866-345-3454; Fax: 1-877-977-8077 Zurich Insurance Company Ltd First Canadian Place, 100 King Street West Suite 5500, P.O. Box 290 Toronto, ON M5X 1C9

Zurich Vendor Panel & Benefits

Zurich has a list of preferred vendors, which includes:

- IT Forensics firms
- Ransom negotiators
- Public relations firms
- Credit monitoring firms/call centers
- Defence counsels

Benefits include:

- Vendors are all experts in their fields
- Access to better rates

Cyber Claims Process

STEP 1: NOTIFY ZURICH

STEP 2: FIRST CONTACT

STEP 3: DETERMINE WHO NEEDS TO GET INVOLVED

STEP 4: ONGOING COMMUNICATION

STEP 5: SUBMIT THE PROOF OF LOSS

STEP 6: FINALIZATION

Questions?

Stay connected | nortonrosefulbright.com/tech

Blogs

- **Data Protection Report** | Provides thought leadership on emerging privacy, data protection and cybersecurity issues | Subscribe
- **Inside Tech Law** | Provides insights, analysis and trends | Subscribe
- **Inside FinTech** | Provides FinTech-related legal, regulatory and topical updates from across the globe | Subscribe

Podcasts

- ***Disputed*** | Conversations will bring both a global perspective and a litigator's instinct for issue spotting to keep your business risk-ready | Listen and subscribe
- **FinTech Pulse** | We explore the latest global news, regulatory developments, trends and hot topics in the Fintech sector | Listen and subscribe

Law around the world

nortonrosefulbright.com

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to 'Norton Rose Fulbright', 'the law firm' and 'legal practice' are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together 'Norton Rose Fulbright entity/entities'). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a 'partner') accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity.

The purpose of this communication is to provide general information of a legal nature. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.