OSLER

# Consumer data: Lessons learned from the security incident trenches

**NOVEMBER 20, 2017 1 MIN READ**

## Related Expertise

- Class Action Defence
- Corporate and Commercial Disputes
- Privacy and Data Management

Authors: Adam Kardash, Brian Thiessen, KC

All businesses that collect and maintain consumer data are facing a rapidly evolving and sophisticated array of security threats to their data holdings, and increasing exposure to legal liability and reputational harm. Your organization's initial response to a security incident is critical in determining the long-term impact the incident will have on your business. The immediate steps you take after a breach can set the tone for the response, influence how smoothly your organization can move forward from the event and affect the risk of privacy, consumer and other class actions and litigation.

## Top 5 priorities when you have a security incident

### Contain
- Take immediate steps to identify and contain the breach
- Assemble breach team
- Do not compromise ability to investigate

### Investigate
- Preliminary investigation
- Longer-term forensic investigation

### Communicate
- Immediate response
- Longer-term outreach

### Notify
- Notification to regulators
- Notification to individuals
- Notification to stakeholders

### Remediate
- Take steps to remediate harm to affected parties

## Key elements of an incident response protocol

- Establishment of a workable protocol and reporting structure
- Identification of service providers and other key stakeholders
- Implementation of steps to protect confidentiality and privilege
- Availability of insurance
- Value of tabletop preparedness testing

## Top 10 best practices for maintaining privilege during security incidents

1. Engage counsel to quarterback the investigation
2. Implement a document freeze
3. Copy counsel on internal and third-party communications
4. Mark documents "privileged and confidential"
5. Forward requests from third parties to counsel where appropriate
6. Establish segregated confidential files
7. Limit circulation of legal advice and privileged reports
8. Retain and manage expert witnesses through counsel
9. Advise team members that purpose of investigation is to obtain legal advice
10. Final report from team leader to counsel

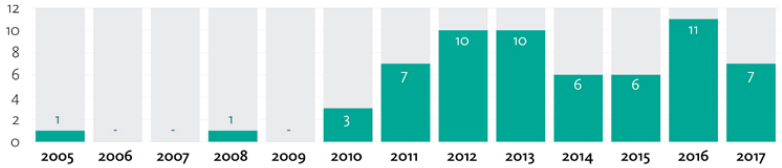
## Risk of privacy class actions brought by consumers

**Key points:**

- Number of privacy class actions initiated by consumers has increased rapidly in recent years
- Hacking is the leading cause of incidents that result in these actions
- Misuse of information and theft/loss of physical media are also leading risks
- Technology/media companies and health care providers have been most frequently hit

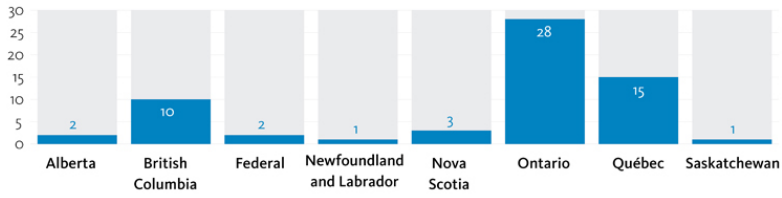
### Number of privacy class actions by year

Grand total: 62



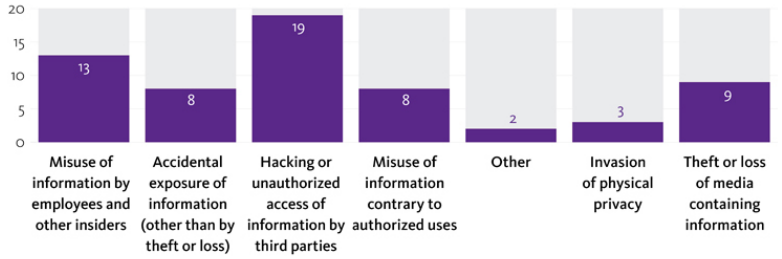

### Number of privacy class actions by jurisdiction

Grand total: 62




### Number of privacy class actions by type of incident

Grand total: 62



## Top 5 priorities when you have a security incident

### Contain
- Take immediate steps to identify and contain the breach
- Assemble breach team
- Do not compromise ability to investigate

### Investigate
- Preliminary investigation
- Longer-term forensic investigation

### Communicate
- Immediate response
- Longer-term outreach

### Notify
- Notification to regulators
- Notification to individuals
- Notification to stakeholders

### Remediate
- Take steps to remediate harm to affected parties

## Key elements of an incident response protocol

- Establishment of a workable protocol and reporting structure
- Identification of service providers and other key stakeholders
- Implementation of steps to protect confidentiality and privilege
- Availability of insurance
- Value of tabletop preparedness testing

## Top 10 best practices for maintaining privilege during security incidents

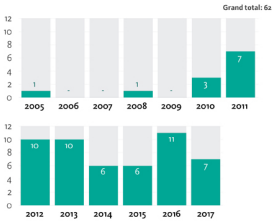
1. Engage counsel to quarterback the investigation
2. Implement a document freeze
3. Copy counsel on internal and third-party communications
4. Mark documents "privileged and confidential"
5. Forward requests from third parties to counsel where appropriate
6. Establish segregated confidential files
7. Limit circulation of legal advice and privileged reports
8. Retain and manage expert witnesses through counsel
9. Advise team members that purpose of investigation is to obtain legal advice
10. Final report from team leader to counsel

## Risk of privacy class actions brought by consumers

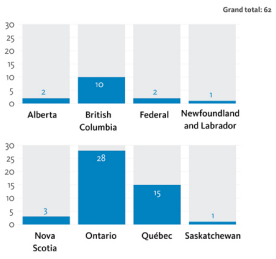
**Key points:**

- Number of privacy class actions initiated by consumers has increased rapidly in recent years
- Hacking is the leading cause of incidents that result in these actions
- Misuse of information and theft/loss of physical media are also leading risks
- Technology/media companies and health care providers have been most frequently hit

### Number of privacy class actions by year




### Number of privacy class actions by jurisdiction




### Number of privacy class actions by type of incident