PIPA BREACH REPORT 2022

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Alberta

410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca

Twitter: @ABoipc

www.oipc.ab.ca

July 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Mandatory breach reporting came into force on May 1, 2010 under Alberta's *Personal Information Protection Act* (PIPA, section 34.1).

Between 2010-2011 and 2020-2021, the Office of the Information and Privacy Commissioner (OIPC) received 1,977 breach reports (or notices) from organizations.[1]

The number of breach reports received each year has increased overall. There were 377 breach reports submitted to the OIPC in 2020-2021, compared with 50 in 2010-2011. This suggests more organizations recognize the importance of responding to privacy breaches, and are aware of the requirement to report certain breaches to the OIPC and to notify affected individuals. The increase may also suggest there are more breaches occurring.

Decisions Issued

The Commissioner has authority under section 37.1 of PIPA to require an organization to notify affected individuals for whom there is a real risk of significant harm as a result of a breach. The Commissioner or a delegate reviews all breach reports and a decision is issued. There are three kinds of decisions or findings:

- Real Risk of Significant Harm (RROSH)
- No Real Risk of Significant Harm (NO RROSH)
- No Jurisdiction

Overall, 1,953 decisions were issued between 2010-2011 and 2020-2021.[2]

Of these, 1,334 were RROSH decisions, representing 68% of all decisions. Between 2017-2018 and 2020-2021, 70% to 80% of decisions were RROSH. In contrast, from 2010-2011 to 2012-2013, less than half were RROSH decisions. When comparing percentages of yearly totals, there is relatively less over-reporting of breaches by organizations. This suggests that organizations have become better at assessing the likelihood of a real risk of significant harm resulting from a breach.

There were 419 NO RROSH decisions issued between 2010-2011 and 2020-2021, representing 22% of all decisions. There were 200 findings of No Jurisdiction, representing 10% of all decisions.

1 The OIPC's fiscal years are from April 1 to March 31. In this report, a "year" describes a fiscal year.

2 At the time of this report, of the 1,977 breach reports received up to March 31, 2021, decisions had been issued for 1,953 of them.

Type of Breach

Breach means a "loss of or unauthorized access to or disclosure of" personal information.

Of the 1,953 breach decisions issued, 42% involved unauthorized access to personal information, 36% involved unauthorized disclosure of personal information and 21% involved a loss of personal information.[3]

As a percentage of yearly totals, in recent years there have been more breaches involving unauthorized access to personal information. This trend aligns with the increase in compromised electronic information systems, described below.

In 2010-2011, approximately 25% of RROSH decisions involved unauthorized access to personal information. In recent years, more than 50% of RROSH decisions involved unauthorized access.

In contrast, 50% of RROSH decisions in 2010-2011 involved a loss of personal information, and in recent years approximately 25% of RROSH decisions involved a loss of personal information.

Unauthorized disclosures of personal information have consistently accounted for approximately 25% of RROSH decisions issued each year.

Of the NO RROSH decisions issued, 78% involved unauthorized disclosure of personal information, with the primary cause being transmission errors, 13% involved a loss of personal information, and 9% involved unauthorized access to personal information.

Breach Causes

Compromised electronic information systems are the most common cause of breaches. Overall, 500 breaches, or 37% of all RROSH decisions issued since 2010-2011, were caused by compromised electronic information systems. A compromised electronic information system includes breaches caused by the installation of malicious software (malware) or ransomware, exploitation of vulnerabilities, through forced intrusions (hacking), or a combination of factors. Compromised electronic information systems may lead to the exfiltration of personal information in digital formats.

The second leading cause is theft. Overall, 204 breaches, or 15% of all RROSH decisions issued, were caused by theft. Theft refers to stolen physical objects, like documents, mobile devices or portable storage media containing personal information.

The third leading cause is transmission errors. Overall, 197 breaches, or 15% of RROSH decisions issued, were caused by transmission errors. Transmission errors most commonly include misdirected mail, emails or faxes.

The fourth leading cause is social engineering and phishing. Overall, 160 breaches, or 12% of RROSH decisions, were caused by social engineering and phishing. In recent years, this has been the second leading cause of breaches, trailing compromised electronic information systems. Phishing is a type of social engineering attack carried out via electronic communications, typically email, but also instant messaging, text messaging and phone calls. The objective of phishing attacks is for perpetrators to get individuals to divulge information for malicious purposes. Social engineering may also occur, for example, when a malicious actor poses as an individual in a conversation with a call centre employee to gain access to the individual's account details with an organization.

Notably, social engineering and phishing often lead to compromised electronic information systems. Social engineering or phishing is captured as the root cause of a privacy breach when reported by the organization. If the organization only

3 Other types of breaches accounted for the remaining 1%. This includes non-jurisdiction findings when a breach did not occur.

reports a compromised electronic information system, but does not report the specific cause, the breach is recorded as a compromised electronic information system. As a result, there are likely more breaches caused by social engineering or phishing than has been reported by organizations.

The fifth leading cause of RROSH breaches is failure to secure. Failure to secure includes when an error, such as a misconfigured website, server or network drive, leaves personal information publicly exposed online, an unencrypted storage medium is lost, or hard copy documents are lost.

Other causes of RROSH decisions include when personal information is published accidentally, when it is misplaced or lost, or when rogue employees cause breaches. Overall, 132 breaches, or 10% of RROSH decisions, had other causes.

Some important reminders after reviewing RROSH decisions:

- Implement regular and/or immediate security patching on networks, servers and devices.
- Sign up for and review updates from cybersecurity agencies and other professionals to keep up to date on new threats and possible solutions to protect the organization's IT infrastructure.
- Train staff regularly on detecting phishing or social engineering attempts.
- Train staff regularly on protecting personal information contained in laptops or paper documents. For example, repeat the message that no devices or documents should be left in vehicles to reduce breaches caused by theft.

For NO RROSH decisions, transmission errors are the most common type of breach. Overall, 260 breaches, or 62% of NO RROSH decisions, were the result of transmission errors. Most NO RROSH breaches are accidental. Errant email is the leading reason for transmission errors, followed by mailing errors. Most commonly, these errors result when an individual's personal information is sent to an incorrect recipient, or the correct recipient receives their personal information but also that of another individual. These types of breaches are discovered relatively quickly, since the sender, recipient or both easily detect the error.

The reasons for No Jurisdiction include when:

- There is no collection, use or disclosure of personal information within Alberta
- What is reported by the organization is determined not to be a breach
- The organization is regulated as a "federal work, undertaking or business"
- The organization is determined not to have had control of the personal information
- The organization is a non-profit organization, and the personal information at issue was not collected, used or disclosed in connection with a commercial activity

Days to Discover

For RROSH decisions, the number of days to discover the breach has increased overall.

Organizations tend to discover transmission errors quickly, as well as breaches involving theft or loss. These types of breaches usually have tangible and perceptible consequences.

Compromised electronic information systems can be insidious and not immediately detectable or observable. Even when one is detected, many organizations report approximate start dates of the breach. For example, if an unauthorized individual gains

access to an employee's email account the employee may not detect suspicious activity, and an investigation may not determine the exact date of when the account was compromised.

In contrast, most NO RROSH decisions are transmission errors, which are discovered quickly.

Days to Report

For RROSH decisions, the number of days to discover the breach has increased overall.

Several factors may contribute to the increase in the length of time it takes for organizations to report breaches to the OIPC. For example, breaches caused by compromised electronic information systems can be more complex and may take longer to investigate. In many cases, organizations are retaining specialized third parties to assist with breach investigation and response, and organizations must now also report to several other regulators in various jurisdictions in Canada, USA or elsewhere. Some of those jurisdictions also require reporting within a specified timeframe, whereas PIPA does not.

Regardless of the underlying reasons for the additional time it takes organizations to report privacy breaches to the OIPC, there is cause for concern for individuals affected. Time is of the essence to mitigate a real risk of significant harm when an individual is affected by a breach.

Industries Affected

In the early years of breach reporting, five industries — Finance; Health Care and Social Assistance; Information; Mining, Quarrying, and Oil and Gas Extraction; and Real Estate and Rental and Leasing — submitted the majority of breach reports. Over time, the disparity among sectors has narrowed significantly. The top reporting industries are reporting at relatively the same rate and nearly all industries have reported breaches.

Retail Trade and Accommodation and Food Services have seen significant increases in breach reports. In these industries, the increase in privacy breaches is almost exclusively due to compromised electronic information systems. This is likely a result of increased reliance on online transactions, such as online purchases or reservations.

Since they are mostly due to human error – and overwhelmingly, transmission errors – NO RROSH breaches are associated with organizations that routinely send information to individuals, primarily the Finance and Insurance industries.

Affected Individuals and Personal Information

The individuals most commonly affected by a RROSH breach are customers or clients (involved in 56% of reported RROSH breaches). Employees are the second most affected group.

Almost all RROSH decisions (between 69% and 81%) involve some basic contact information, such as telephone number or mailing address, in association with an individual's name.

Most RROSH decisions also involve identity, financial and employment information.

In recent years, email addresses have been increasingly involved in RROSH breaches, while the prevalence of medical information has decreased. The increase in the percentage of breaches that involve transaction information, such as purchase history, reflects the increase in breaches that result from compromised electronic information systems, especially e-commerce websites.

Harm

The types of harm arising from breach reports largely reflect the evolving causes of breaches and the personal information at issue in these breaches. Identity theft, fraud and risk of financial loss have been constants. More recently, phishing as a harm has been increasing, as more reported breaches involve stolen or compromised email addresses.

Of RROSH decisions, 71% were found to be caused by deliberate action or malicious intent (that is, they are not accidental). This includes ransomware attacks, system hacks, theft, phishing and deliberate action by rogue employees. The majority of RROSH breaches for which there was no deliberate action are unauthorized disclosures.

Of NO RROSH decisions, 86% were found to be caused inadvertently or accidentally.

Also noted in many RROSH decisions was the personal information at issue was not recovered, returned or securely destroyed. For example, for RROSH decisions where the cause was accidental, the risk of harm increases when the recipient has a personal or professional relationship with the affected individual, or the recipient does not return or confirm deletion of the personal information.

Another factor in analyzing "significant harm" is the length of time that the personal information is exposed, particularly when personal information is exposed through a compromised electronic information system.

Number of Affected Individuals

Of the 1,334 RROSH decisions issued during the period, 1,244 included information about the total number of affected individuals whose personal information was collected in Alberta and notification to them was required.[4] In 90 decisions, the reporting organization did not provide or was not able to confirm the exact number of affected individuals whose information was collected, used or disclosed in Alberta.

There is no discernable trend from year to year regarding the number of notices to affected individuals. In 2010-2011, 1,821 notifications were required as a result of breaches under PIPA, and in 2020-2021, 1,951,180 notifications were required.

Number of Days to Notify Affected Individuals

Section 37.1(7) of PIPA says, "Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information."

In 2010-2011, organizations had already notified affected individuals in approximately 55% of breaches reported to the OIPC. Since 2012-2013, at least 80% of organizations had already notified affected individuals at the time the breach was reported to the Commissioner.

Overall, each year, it took on average between 18 and 54 days for organizations to notify affected individuals, with no discernable trend from year to year.

Breaches that involved "loss" and "unauthorized disclosure" have similar averages (37 and 39 days), while breaches involving "unauthorized access" had a higher average (55 days), and this was particularly the case from 2018-2019 to 2020-2021. The difference correlates with compromised electronic information systems often being difficult to discover and investigate.

4 The number of affected individuals is based on what organizations report, and there is often no distinction made between Alberta residents and individuals whose information was collected, used or disclosed in Alberta.

Type of Notification

Section 19.1(1) of the PIPA Regulation requires organizations to notify affected individuals directly; however, notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

In 91% (1,222) of RROSH decisions, organizations notified affected individuals directly, including by in-person meetings, telephone, mail or email.

In 4% (60) of RROSH decisions, the Commissioner authorized indirect notification. In 52 of those cases, the organization also notified some individuals directly. Authorization of indirect notification most commonly occurred when the organization did not have current contact information for all or some of the affected individuals.

Organizations notified individuals indirectly using website postings, social media or traditional media.

The type of notification was unknown in the remaining 4% of RROSH decisions.

Method of Notification

PIPA does not prescribe or restrict the method of notification.

Most individuals are notified by mail. In recent years, relatively more people have been notified by email and telephone.

The increase in notification by electronic means may be in part due to the increased use of email between individuals and organizations, the speed of delivery, and cost considerations. It may also be that organizations only have email addresses of customers, so email is the only available method of notification.

Criteria for RROSH

The factors that contribute to RROSH decisions include:

- Deliberate action or malicious intent to cause the breach
- Personal information was not recovered, returned or destroyed securely
- Length of time the personal information was exposed
- Personal information was exposed and no auditing or ability to determine whether information was accessed
- No encryption of personal information

Criteria for NO RROSH

The factors that contribute to NO RROSH decisions include:

- Accidental or inadvertent cause of the breach
- Personal information is recovered, the organization confirms it has been destroyed securely, or the organization confirms it has not been used, forwarded or retained
- Encryption of the personal information
- Breach is reported to the organization by the unintended recipient(s)
- Unintended recipient of personal information is a known or trusted party
- Fewer personal information data elements are at issue, and the personal information cannot be used to cause significant harm

INTRODUCTION

Alberta's *Personal Information Protection Act* (PIPA or the Act) came into force on January 1, 2004.[5] PIPA applies to "organizations" defined in section 1(1)(i)), in respect of the collection, use, disclosure and safeguarding of "personal information" (defined in section 1(1)(k)).

PIPA was amended in May 2010 to include mandatory breach reporting provisions. The amendments resulted from a review of the Act by the all-party Select Special Personal Information Protection Act Review Committee of the Legislative Assembly (the committee).

As part of its review, the committee issued a discussion guide and conducted a public consultation. The discussion guide asked for input on a potential breach reporting and notification scheme under PIPA. The committee received 65 written submissions in total, and heard 10 oral presentations from organizations, individuals, the Government of Alberta and the Office of the Information and Privacy Commissioner (OIPC) during the review process.

OIPC Submission to PIPA Review Committee

In its November 2006 submission to the committee, the OIPC proposed a number of amendments to "further enhance and strengthen" PIPA, including to:

> Amend PIPA to require organizations to report personal information security breaches that meet pre-established criteria to the Commissioner. Such criteria should include:
>
> - the type of personal information involved in the breach and the reasonable likelihood of material harm to individuals as a result of the breach
> - the likelihood that the personal information has been acquired by unauthorized individuals
> - the likelihood that the personal information can be used by unauthorized individuals (i.e. was the information encrypted, or otherwise inaccessible)
>
> ...
>
> Amend the Act to give the Commissioner the explicit power to order organizations to notify individuals affected by an information security breach, where the organization's risk assessment and consultation with the OIPC concludes there is a reasonable likelihood of material harm to affected individuals. Although this power is not expected to be used often, it is imperative that the Commissioner have the ability to compel notification.

5 *Personal Information Protection Act*, SA 2003, c P-6.5.

In making these recommendations, the OIPC noted:

> PIPA requires that organizations implement reasonable safeguards to protect personal information in their custody or control from such risks as unauthorized use, disclosure and access. Proactive implementation of safeguards is the most effective way to protect individuals from the potential harm resulting from unauthorized access to their personal information.
>
> Nonetheless, security breaches do occur, even where organizations have implemented reasonable safeguards.

The OIPC's submission also recognized the negative impact breaches can have on individuals, including financial loss or fraud, and the need to act quickly in the event of a breach to reduce the risk of harm arising. The OIPC said:

> Individuals must act quickly to minimize the damages that can be incurred from unauthorized access, acquisition and possible misuse of their personal information. Timely notification is imperative. If individuals are not aware that their information has been exposed, they will be unable to protect themselves or mitigate impact in a timely way. Individuals have a fundamental right to know if they have been exposed to such risks.

The OIPC did not, however, recommend mandatory breach notification to individuals for all breaches:

> Notification may not be appropriate in all circumstances. Mandatory notification of breaches in all cases may result in individuals becoming desensitized to such notices. Where there is no reasonable risk or likelihood of material harm to the individual, notification may only serve to raise unwarranted fear or anxiety...
>
> Given the myriad of factors that must be considered in deciding when and how to notify individuals affected by an information security breach, the OIPC is not recommending a mandatory provision requiring organizations to notify individuals.

Instead, the OIPC recommended that breaches be reported to the OIPC to "allow the OIPC an opportunity to work with the organization to determine if notification of individuals is required and, if so, the most appropriate means of doing so."

PIPA Review Committee Final Report

In November 2007, the committee submitted its final report to government, with 39 recommendations for amendments to PIPA.

With respect to breach reporting and notification, the committee made two recommendations.

The committee said, "Privacy breaches can have serious consequences for individuals, ranging from humiliation and anxiety to the use of personal information for criminal purposes, such as fraud" and "are matters of great concern to privacy commissioners and the public." The committee also considered several factors such as "notification fatigue" for individuals affected by privacy breaches, "risk of harm" as a threshold for triggering breach notification and "administrative burdens on organizations" in making the following recommendation:

- That the Act be amended to require organizations to notify the Office of the Information and Privacy Commissioner of a privacy breach involving personal information if the privacy breach meets certain criteria, and to notify affected individuals if directed to do so by the Commissioner, subject to the condition that there is an expedited process where notifying the individual is time-critical...

Additionally, the committee reviewed the Commissioner's power to order an organization to comply with any duty under PIPA, and noted that "without a new offence provision for the failure to notify, it would be an offence only if an organization ignored a Commissioner's order to notify." Therefore, the committee also recommended:

- That the Act be amended to make it an offence not to notify the Office of the Information and Privacy Commissioner of a security breach affecting personal information, where it is reasonable to do so.

In October 2009, the government introduced amendments to PIPA, including:

- Privacy breach reporting and notification requirements
- The power for the Commissioner to require organizations to notify individuals affected by a privacy breach in certain circumstances
- A new offence provision for failure to notify the Commissioner of a privacy breach

The amendments passed in November 2009 and, along with supporting regulations, came into force on May 1, 2010.

Reporting and Notification Provisions[6]

Section 34.1 of PIPA reads as follows:

> 34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.
>
> (2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

A notice provided to the Commissioner under section 34.1(1) of PIPA must include the information prescribed by section 19 of the *Personal Information Protection Act Regulation* (PIPA Regulation). Section 19 of the PIPA Regulation states the notice must be in writing and include the following information:

- A description of the circumstances of the breach[7]
- The date on which or time period during which the breach occurred
- A description of the personal information involved in the breach
- An assessment of the risk of harm to individuals as a result of the breach
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the breach

6 Appendix A sets out the breach reporting and notification provisions as written in legislation.

7 "Breach" means "loss of or unauthorized access to or disclosure of" personal information.

- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the breach
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the breach

It is an offence for an organization to fail to notify the Commissioner of a reportable breach under section 34.1 of PIPA (section 59(1)(e.1)). If guilty of an offence, an individual is subject to a fine up to $10,000 and any other person to a fine up to $100,000 (section 59(2)).

When notifying individuals affected by a breach, section 19.1 of the PIPA Regulation states that the notice must be given directly to the individual and include:

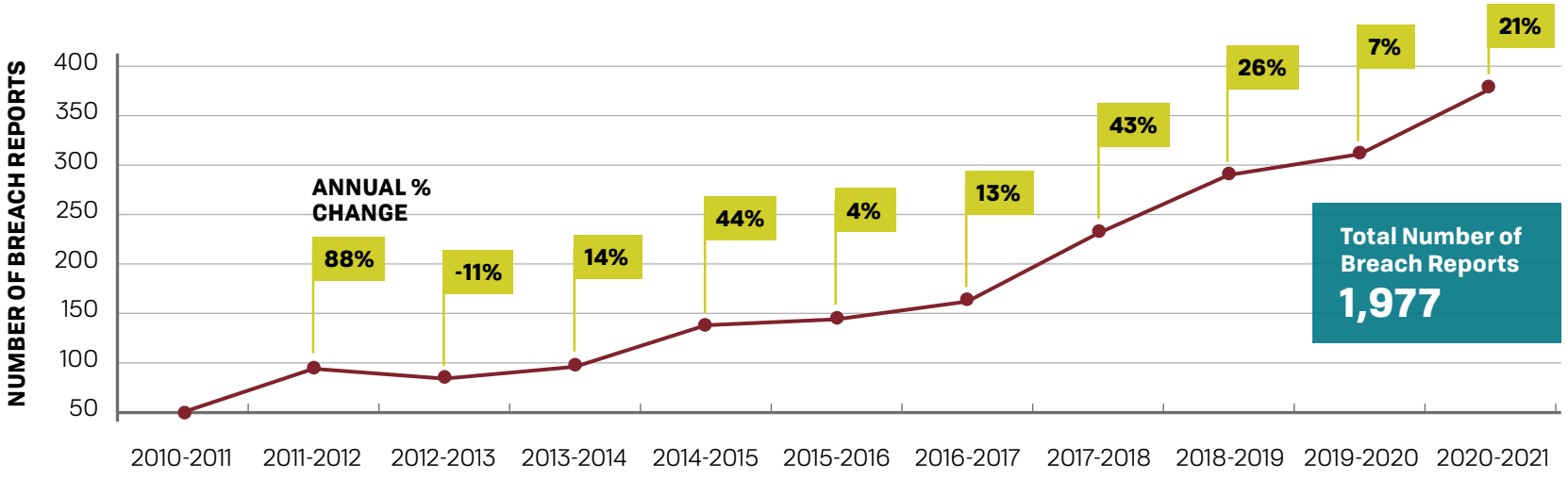
- A description of the circumstances of the breach
- The date on which or time period during which the breach occurred
- A description of the personal information involved in the breach
- A description of any steps the organization has taken to reduce the risk of harm
- The name and contact information for a person who can answer, on behalf of the organization, questions about the breach

Section 37.1(7) of PIPA states that an organization is not prohibited or restricted from notifying individuals on its own initiative. When notifying individuals on their own accord, organizations are encouraged to notify individuals in the form prescribed by the PIPA Regulation to avoid the potential of having to re-notify affected individuals should the Commissioner require notification under section 37.1. The Commissioner will require organizations to re-notify affected individuals where the prior notification issued by the organization did not meet the requirements of the PIPA Regulation.

BREACH REPORTS

Between April 1, 2010 and March 31, 2021, the OIPC received 1,977 notices to the Commissioner under section 34.1 of PIPA. The OIPC refers to these notices as "breach reports" or "self-reported breaches".[8]

FIGURE 1: Number of Breach Reports Received



There were 50 breach reports received in 2010-2011 and 377 breach reports in 2020-2021. These numbers suggest increased organizational awareness about the importance of responding to privacy breaches, and about the requirement to report certain breaches to privacy regulators and to notify affected individuals. The numbers may indicate that more breaches are occurring.

8 The OIPC has changed its breach report form and decision format, which resulted in some variations in the details collected for each breach report.

Decisions Issued

Where an organization experiences a breach that the organization is required to report under section 34.1, the Commissioner has authority under section 37.1 of PIPA to require the organization to notify affected individuals to whom there is a real risk of significant harm as a result of the breach.

All notices provided to the OIPC are reviewed by the Commissioner or a delegate, and a decision is issued. There are three kinds of decisions or findings:

- Real Risk of Significant Harm (RROSH)
- No Real Risk of Significant Harm (NO RROSH)
- No Jurisdiction

For the breach reports received up to March 31, 2021, there were 1,953 decisions issued.

FIGURE 2: Type of Decision by Year

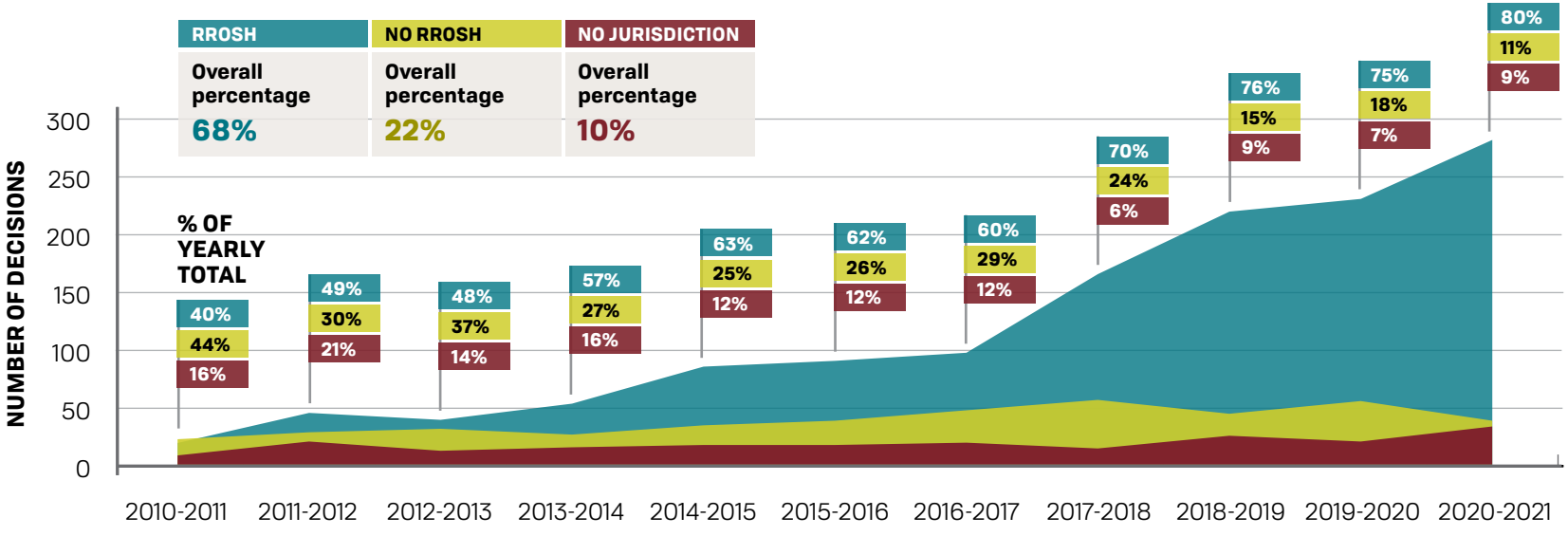


TABLE 1: Type of Decision by Year

TYPE OF DECISION	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
RROSH	20	46	40	54	86	91	98	166	220	231	282	**1,334**
NO RROSH	22	28	31	26	34	38	47	56	44	55	38	**419**
No Jurisdiction	8	20	12	15	17	17	19	14	25	20	33	**200**
Total	**50**	**94**	**83**	**95**	**137**	**146**	**164**	**236**	**289**	**306**	**353**	**1,953**

Overall, 68% of breaches for which decisions have been issued were determined to be RROSH.

There has been a significant change over the period. The number of RROSH decisions as a percentage of yearly total has increased overall. Only 40% of decisions were RROSH in 2010-2011 compared with 80% in 2020-2021.

The number of NO RROSH decisions as a percentage of yearly total has decreased overall. In 2010-2011, 44% of decisions resulted in NO RROSH compared with 11% in 2020-2021.

The number of No Jurisdiction findings as a percentage of yearly total has also decreased overall, with less than 10% each year since 2016-2017.

These stats suggest increased sophistication by organizations in assessing the likelihood of significant harm resulting from a breach, resulting in less over-reporting of breaches.

Type of Breach

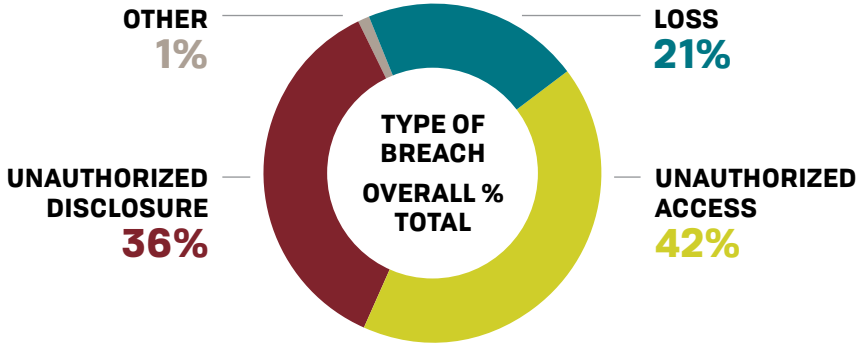
Section 34.1 of PIPA requires organizations to notify the Commissioner of "any incident involving the **loss of or unauthorized access to or disclosure of the personal information** where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" [emphasis added].

Of the 1,953 breach decisions issued, 42% involved unauthorized access to personal information, 36% involved unauthorized disclosure of personal information and 21% involved a loss of personal information.

As a percentage of yearly totals, in recent years there have been more breaches involving unauthorized access to personal information. This change aligns with the increase in compromised electronic information systems, described below.

TABLE 2: All Cases – Type of Breach – Number of Decisions by Year and Percent of Decisions as Yearly Total

TYPE OF BREACH	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Loss	21	32	22	23	27	38	37	41	65	66	44	**416**
% of Yearly Total	42%	34%	27%	24%	20%	26%	23%	17%	22%	22%	12%	**21%**
Unauthorized Access	9	26	18	34	38	59	62	108	123	129	216	**822**
% of Yearly Total	18%	28%	22%	36%	28%	40%	38%	46%	43%	42%	61%	**42%**
Unauthorized Disclosure	20	36	43	37	70	48	63	86	94	109	89	**695**
% of Yearly Total	40%	38%	52%	39%	51%	33%	38%	36%	33%	36%	25%	**36%**
Other	0	0	0	1	2	1	2	1	7	2	4	**20**
% of Yearly Total	0%	0%	0%	1%	1%	1%	1%	0%	2%	1%	1%	**1%**
Number of Decisions Total	**50**	**94**	**83**	**95**	**137**	**146**	**164**	**236**	**289**	**306**	**353**	**1,953**



Cause of Breach

The main causes of reported breaches are compromised electronic information systems, transmission errors and thefts.

TABLE 3: All Cases – Breach Cause – Number of Decisions by Year

BREACH CAUSE	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Compromised Electronic Information System	4	21	15	26	25	43	57	96	78	78	151	**594**
Transmission Error	14	21	29	22	34	34	50	67	69	76	65	**481**
Theft	14	19	11	18	19	29	19	23	36	39	32	**259**
Failure to Secure	5	13	12	4	28	8	7	14	33	40	36	**200**
Social Engineering / Phishing	1	2	1	3	4	10	8	11	36	47	55	**178**
Other	11	18	15	17	25	21	19	23	30	23	9	**211**
Unknown	1	0	0	5	2	1	4	2	7	3	5	**30**
Total	**50**	**94**	**83**	**95**	**137**	**146**	**164**	**236**	**289**	**306**	**353**	**1,953**

The number of breach reports involving compromised electronic information systems has increased significantly overall. In 2020-2021, for example, 151 breaches involving compromised electronic information systems were reported, compared with 4 in 2010-2011. There has also been an overall increase in the number of breach reports involving social engineering or phishing.

The number of breaches involving transmission errors has also increased overall, but there has been a relative decrease in transmission errors as a percentage of yearly total.

Email became the leading cause of transmission errors in recent years, while mail, telephone and fax made up a greater proportion of transmission errors in the early years of mandatory breach reporting.

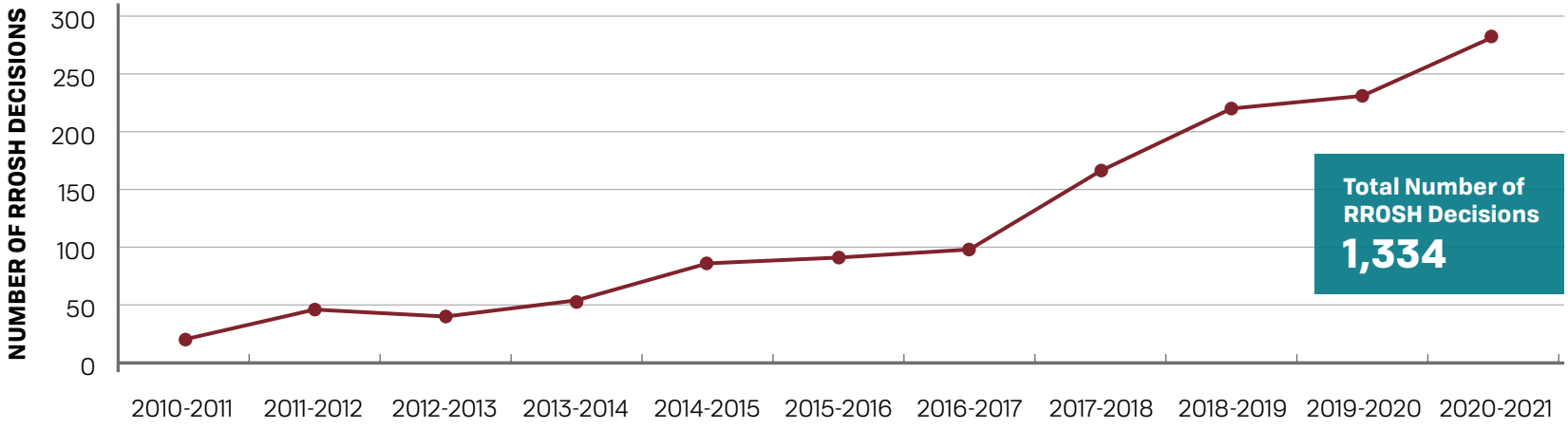
The number of breaches involving theft has remained generally stable, resulting in a decrease of theft as a percentage of yearly total.

RROSH DECISIONS

This section focuses on the characteristics of RROSH decisions.

As described above, the number of reported breaches that result in a RROSH decision has increased overall, with significant increases in recent years.

FIGURE 3: RROSH – Number of Decisions by Year

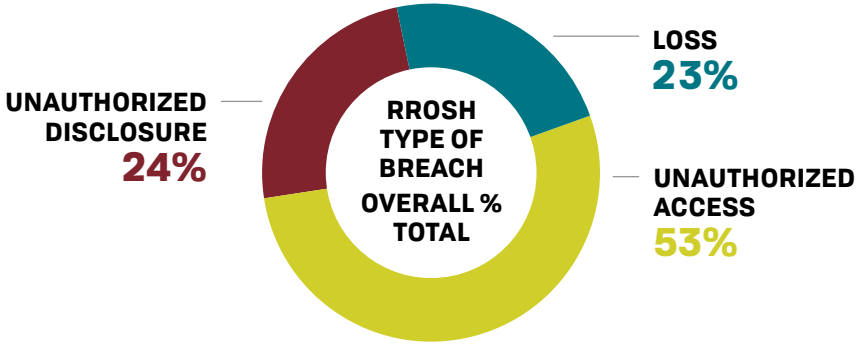


Of 1,953 decisions issued, 68% (1,334) have been RROSH decisions.

Of the 1,334 RROSH decisions, 53% (702) involved unauthorized access to personal information, followed by 23% (314) involving a loss of personal information, and 24% (318) involving unauthorized disclosure of personal information.

TABLE 4: RROSH – Type of Breach – Number of Decisions by Year and Percent of Decisions as Yearly Total

TYPE OF BREACH	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Loss	10	16	16	15	24	28	24	35	55	53	38	**314**
% of Yearly Total	50%	35%	40%	28%	28%	31%	24%	21%	25%	23%	13%	**23%**
Unauthorized Access	5	16	12	25	26	49	53	95	111	116	194	**702**
% of Yearly Total	25%	35%	30%	46%	30%	54%	54%	57%	50%	50%	69%	**53%**
Unauthorized Disclosure	5	14	12	14	36	14	21	36	54	62	50	**318**
% of Yearly Total	25%	30%	30%	26%	42%	15%	21%	22%	25%	27%	18%	**24%**
Number of Decisions Total	**20**	**46**	**40**	**54**	**86**	**91**	**98**	**166**	**220**	**231**	**282**	**1,334**



Fully 50% of decisions issued for breaches reported in 2010-2011 related to a loss of personal information, whereas unauthorized access and disclosure accounted for approximately 25% each.

In recent years, RROSH decisions involved unauthorized access in over 50% of cases, and loss of personal information accounted for approximately 25% of RROSH decisions issued.

Unauthorized disclosures of personal information have consistently accounted for approximately 25% of RROSH decisions issued each year.

Causes of RROSH Breaches

The main causes of breaches that result in a RROSH decision are compromised electronic information systems, transmission errors and theft.

TABLE 5: RROSH – Breach Cause – Number of Decisions by Year

BREACH CAUSE	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
Compromised Electronic Information System	3	15	9	21	21	37	49	83	63	67	132	**500**	**37%**
Transmission Error	3	8	7	7	6	10	15	29	39	42	31	**197**	**15%**
Theft	9	11	9	11	16	20	12	22	32	33	29	**204**	**15%**
Failure to Secure	2	8	5	3	26*	1	3	5	25	24	30	**132**	**10%**
Social Engineering / Phishing	0	1	1	1	3	7	6	11	34	44	52	**160**	**12%**
Unknown	0	0	0	1	0	0	2	0	1	2	3	**9**	**1%**
Other	3	3	9	10	14	16	11	16	26	19	5	**132**	**10%**
Total	**20**	**46**	**40**	**54**	**86**	**91**	**98**	**166**	**220**	**231**	**282**	**1334**	

*The higher value in this year is due to a single breach affecting 21 organizations (plus additional organizations the following year).

With the exception of 2014-2015, compromised electronic information systems have been the leading cause of RROSH breaches since 2011-2012.

There has been a steady increase in the number of social engineering and phishing breaches. Social engineering and phishing breaches were the second leading cause of RROSH breaches in 2019-2020 and 2020-2021.

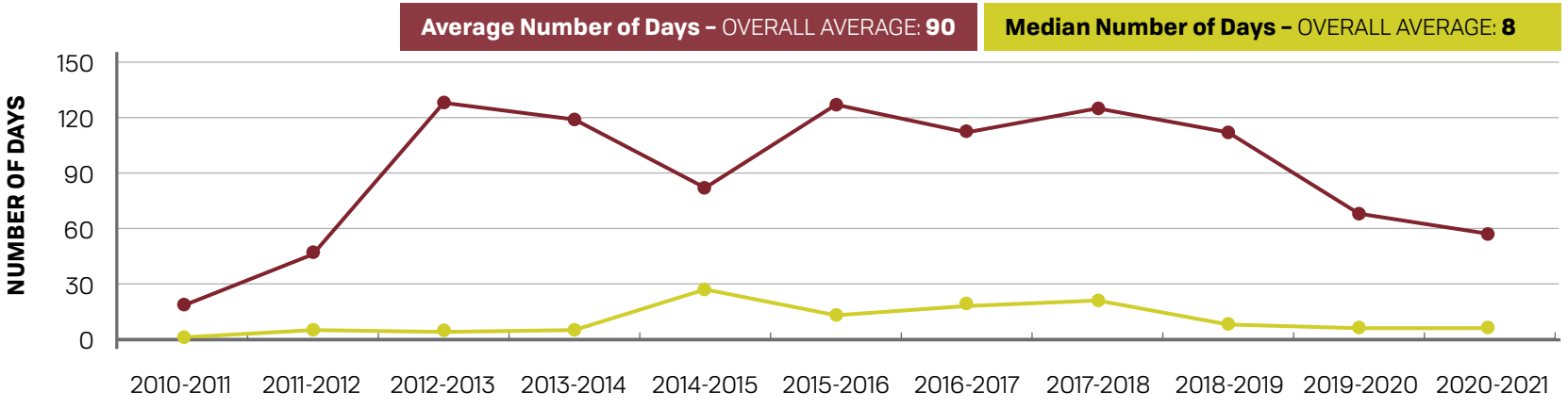
Social engineering and phishing often lead to compromised electronic information systems. Social engineering or phishing is captured as the root cause of a privacy breach when reported by the organization. If the organization only reports a compromised electronic information system, but does not report the specific cause, the breach is recorded as a compromised electronic information system. As a result, there are likely more breaches caused by social engineering or phishing than has been reported by organizations.

Timelines – Days to Discover[9]

Overall, 45% of RROSH breaches are discovered in less than 7 days, 22% are discovered in 7 to 60 days, and 25% are discovered in more than 60 days, with 8% unknown.

TABLE 6 and FIGURE 4: RROSH – Days to Discover – Number of Decisions by Year

DAYS TO DISCOVER	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
7 or less	15	26	18	22	26	38	37	64	99	119	139	**603**	**45%**
7 - 14	0	4	3	3	4	4	9	10	13	27	26	**103**	**8%**
14 - 30	1	2	4	2	6	6	7	9	16	12	25	**90**	**7%**
30 - 60	1	3	0	1	5	6	13	13	19	17	10	**88**	**7%**
60 or more	2	8	6	10	30	28	29	59	53	45	67	**337**	**25%**
Unknown	1	3	9	16	15	9	3	11	20	11	15	**113**	**8%**
Total	**20**	**46**	**40**	**54**	**86**	**91**	**98**	**166**	**220**	**231**	**282**	**1,334**	



9 In a number of cases, breach reports received by the OIPC include only approximate dates, not exact dates for when breaches occurred. All approximate dates were updated as follows:

- For start dates, to the first day of the approximate period (usually month or year)
- For end dates, to the last day of the approximate period (usually month or year)
- For breaches that had multiple dates of incidents the entire date range is used. For example, if a breach occurred on February 1 and again on April 5, the breach was deemed to have occurred from February 1 to April 5. This assumption was used for 30 breach reports.

Organizations tend to discover transmission errors quickly, as well as breaches involving theft or loss. These types of breaches usually have tangible and perceptible consequences, such as a transmission error where the mistake can be identified almost immediately by the sender, the recipient or both. Theft and other types of losses of personal information are also often immediately apparent.

Compromised electronic information systems can be insidious and not immediately detectable or observable. Even when one is detected, many organizations report approximate start dates of the breach. For example, if an unauthorized individual gains access to an employee's email account the employee may not detect suspicious activity, and an investigation may not determine the exact date of when the account was compromised.

There is a gap between overall median number of days to discover and average number of days to discover. This shows that certain breaches are discovered long after they have occurred, which significantly affects the average number of days to discover. The median number of days to discover has been less than 30 each year.

Last, as seen in many breach reports involving compromised electronic information systems, even when the breach has been detected, some organizations report only approximate start dates. This may also affect the average breach durations reported above.

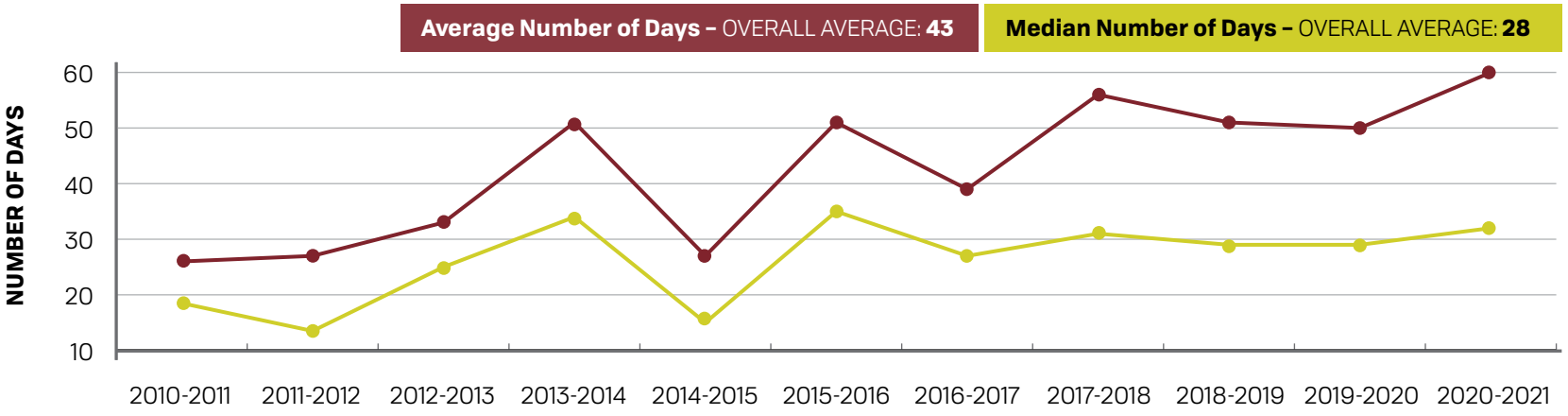
Timelines – Days to Report

With respect to reporting breaches to the OIPC, section 34.1(1) of PIPA requires organizations to provide notice to the Commissioner "without unreasonable delay". The data for RROSH decisions shows a gradual, albeit inconsistent, increase in the number of days to report breaches.

TABLE 7: RROSH – Days to Report – Number of Decisions by Year

DAYS TO REPORT	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
7 or less	5	14	9	8	19	14	16	19	22	40	40	**206**	**15%**
7 - 14	4	12	5	3	16	15	13	21	31	36	40	**196**	**15%**
14 - 30	7	7	9	13	23	15	23	36	58	42	53	**286**	**21%**
30 - 60	2	4	11	13	13	22	35	41	53	54	73	**321**	**24%**
60 or more	2	7	4	12	6	23	10	44	53	59	73	**293**	**22%**
Unknown	0	2	2	5	9	2	1	5	3	0	3	**32**	**2%**
Total	**20**	**46**	**40**	**54**	**86**	**91**	**98**	**166**	**220**	**231**	**282**	**1334**	

FIGURE 5: RROSH – Days to Report – Number of Decisions by Year



Several factors may contribute to the increase in the length of time it takes for organizations to report breaches to the OIPC. For example, breaches caused by compromised electronic information systems can be more complex and may take longer to investigate. In many cases, organizations are retaining specialized third parties to assist with breach investigation and response, and organizations must now also report to several other regulators in various jurisdictions in Canada, USA or elsewhere. Some of those jurisdictions also require reporting within a specified timeframe, whereas PIPA does not.

Regardless of the underlying reasons for the additional time it takes organizations to report privacy breaches to the OIPC, there is cause for concern for individuals affected. Time is of the essence to mitigate a real risk of significant harm when an individual is affected by a breach.

Industry Reporting[10]

In 2010-2011, approximately 75% of breaches determined to be RROSH were spread across five industries:

Finance 25%

Health Care and Social Assistance 20%

Information 10%

Mining, Quarrying, and Oil and Gas Extraction 10%

Real Estate and Rental and Leasing 10%

TABLE 8: RROSH – Industry of Reporting Organization – Number of Decisions by Year and Percent as Yearly Total

INDUSTRY	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Accommodation and Food Services	0 (0%)	2 (4%)	1 (3%)	0 (0%)	1 (1%)	6 (7%)	2 (2%)	17 (10%)	11 (5%)	4 (2%)	4 (1%)	**48 (4%)**
Administrative and Support and Waste Management and Remediation Services	0 (0%)	0 (0%)	2 (5%)	1 (2%)	3 (3%)	0 (0%)	1 (1%)	3 (2%)	5 (2%)	4 (2%)	2 (1%)	**21 (2%)**
Agriculture, Forestry, Fishing and Hunting	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (1%)	0 (0%)	0 (0%)	1 (0%)	**2 (0%)**
Arts, Entertainment, and Recreation	1 (5%)	0 (0%)	0 (0%)	2 (4%)	0 (0%)	2 (2%)	2 (2%)	6 (4%)	7 (3%)	6 (3%)	6 (2%)	**32 (2%)**
Construction	0 (0%)	1 (2%)	1 (3%)	2 (4%)	1 (1%)	2 (2%)	1 (1%)	4 (2%)	5 (2%)	6 (3%)	7 (2%)	**30 (2%)**
Educational Services	0 (0%)	0 (0%)	0 (0%)	1 (2%)	1 (1%)	3 (3%)	2 (2%)	1 (1%)	8 (4%)	0 (0%)	14 (5%)	**30 (2%)**
Finance	5 (25%)	6 (13%)	5 (13%)	8 (15%)	31 (36%)	11 (12%)	18 (18%)	22 (13%)	32 (15%)	41 (18%)	40 (14%)	**219 (16%)**
Insurance	1 (5%)	7 (15%)	7 (18%)	6 (11%)	10 (12%)	8 (9%)	2 (2%)	6 (4%)	21 (10%)	27 (12%)	21 (7%)	**116 (9%)**
Health Care and Social Assistance	4 (20%)	1 (2%)	1 (3%)	2 (4%)	5 (6%)	2 (2%)	5 (5%)	13 (8%)	9 (4%)	10 (4%)	17 (6%)	**69 (5%)**
Information	2 (10%)	5 (11%)	3 (8%)	7 (13%)	7 (8%)	9 (10%)	10 (10%)	13 (8%)	14 (6%)	24 (10%)	17 (6%)	**111 (8%)**
Manufacturing	1 (5%)	2 (4%)	4 (10%)	7 (13%)	2 (2%)	2 (2%)	7 (7%)	12 (7%)	9 (4%)	10 (4%)	30 (11%)	**86 (6%)**

10 The industry categories used in this report are based on the 2017 North American Industry Classification System (NAICS) nomenclature. The only deviation concerns the "Finance and Insurance" category, which was split in two to report statistics.

INDUSTRY	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Mining, Quarrying, and Oil and Gas Extraction	2 (10%)	4 (9%)	2 (5%)	6 (11%)	2 (2%)	5 (5%)	4 (4%)	6 (4%)	9 (4%)	8 (3%)	7 (2%)	**55 (4%)**
Other Services (except Public Administration)	0 (0%)	1 (2%)	5 (13%)	2 (4%)	4 (5%)	8 (9%)	13 (13%)	12 (7%)	26 (12%)	29 (13%)	38 (13%)	**138 (10%)**
Professional, Scientific, and Technical Services	0 (0%)	7 (15%)	3 (8%)	4 (7%)	2 (2%)	5 (5%)	10 (10%)	19 (11%)	15 (7%)	15 (6%)	21 (7%)	**101 (8%)**
Public Administration	0 (0%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (0%)	0 (0%)	**2 (0%)**
Real Estate and Rental and Leasing	2 (10%)	2 (4%)	0 (0%)	0 (0%)	0 (0%)	3 (3%)	4 (4%)	5 (3%)	6 (3%)	5 (2%)	9 (3%)	**36 (3%)**
Retail Trade	0 (0%)	5 (11%)	5 (13%)	4 (7%)	12 (14%)	18 (20%)	14 (14%)	21 (13%)	33 (15%)	23 (10%)	28 (10%)	**163 (12%)**
Transportation and Warehousing	1 (5%)	0 (0%)	0 (0%)	0 (0%)	2 (2%)	3 (3%)	1 (1%)	2 (1%)	4 (2%)	6 (3%)	3 (1%)	**22 (2%)**
Utilities	1 (5%)	0 (0%)	1 (3%)	0 (0%)	0 (0%)	1 (1%)	0 (0%)	0 (0%)	0 (0%)	3 (1%)	3 (1%)	**9 (1%)**
Wholesale Trade	0 (0%)	2 (4%)	0 (0%)	1 (2%)	1 (1%)	3 (3%)	2 (2%)	3 (2%)	4 (2%)	8 (3%)	10 (4%)	**34 (3%)**
Unknown	0 (0%)	0 (0%)	0 (0%)	1 (2%)	2 (2%)	0 (0%)	0 (0%)	0 (0%)	2 (1%)	1 (0%)	4 (1%)	**10 (1%)**

In 2020-2021, the industry sectors reporting RROSH breaches were:

- Finance (14%)
- Other Services (13%) – this category includes mostly not-for-profit organizations, cooperatives and regulatory colleges
- Manufacturing (11%)
- Retail trade (10%)
- Insurance (7%)
- Professional, Scientific, and Technical Services (7%)
- Information (6%)
- Health Care and Social Assistance (6%)
- Educational Services (5%)
- Real Estate and Rental and Leasing (3%)
- The remaining categories (Accommodation and Food Services / Administrative and Support and Waste Management and Remediation Services / Agriculture, / Forestry, Fishing and Hunting / Arts, Entertainment, and Recreation / Construction / Mining, Quarrying, and Oil and Gas Extraction / Public Administration / Transportation and Warehousing / Utilities / Wholesale Trade / unknown) are under 3%.

Over time, the disparity among sectors has narrowed significantly; that is, the top reporting industries are all reporting at relatively the same rate. Further, organizations in almost all industries have reported breaches over the years.

Retail trade has seen a significant increase in reported breaches (from 0 to about 30 breaches per year), as has Accommodation and Food Services (from 0 to a high of 17). In these industry sectors, the increase in privacy breaches is almost exclusively due to compromised electronic information systems. This may be due to the increased reliance on online transactions, such as online purchases or reservations.

Affected Individuals – Type

The individuals most commonly affected by a RROSH breach are customers/clients. They are affected in 56% of reported RROSH breaches. Employees are the second most affected group.

The industry sector reporting the breach appears to be a significant determining factor of the type of individuals affected by a RROSH breach. Personal information of customers/clients is involved in RROSH breaches in all industries where organizations traditionally collect, use, access, or disclose the personal information of individuals (that is, all except Manufacturing and Mining, Quarrying, and Oil and Gas Extraction). Employee information is at issue in breaches reported from all industry sectors.

TABLE 9: RROSH – Types of Individual – Number of Decisions by Year

Note: Each decision may include more than one type of affected individual.

TYPE OF INDIVIDUAL	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL %
Customer / Client	9	34	22	33	39	63	69	113	127	148	151	**56%**
Employee	10	14	13	17	21	25	18	42	59	50	94	**25%**
Member	0	0	2	0	23	7	8	7	21	18	14	**7%**
Relative	1	0	2	1	2	4	0	7	10	2	4	**2%**
Patient	4	0	1	1	2	1	4	5	4	12	10	**3%**
Student	0	1	2	1	2	2	1	0	6	1	2	**1%**
Donor	0	0	0	1	1	0	1	1	1	0	20	**2%**
Other	1	1	1	3	2	1	7	4	8	11	11	**4%**

Personal Information at Issue

The information categories used are as follows:

- **Contact information:** Home address, personal phone number, emergency contact information
- **Identity:** Date of birth, driver's licence number, passport number, personal health number, social insurance number
- **Financial:** Payment card information (number, expiry, security code), banking information (institution, account number, balance, cheque), investment information (account number, balance, investment type, gain or loss), beneficiary
- **Employment:** Salary, pay information, employment performance, employment dates, employee identifier, position, name of employer, occupation, employment history, disability
- **Email address:** Personal email, business email
- **Medical information:** Information about condition, history, health service provider information, health identifier
- **Credentials:** Username, password, security questions, security responses
- **Insurance:** Insurance identifier, policy number, policy information, coverage, premium, insurance claim, beneficiary
- **Other:** The personal information elements that together make up less than 20% of the total number of personal information elements in the dataset were grouped in an "other" category

Almost all RROSH decisions (between 69% and 81%) involved some basic contact information, such as telephone number or mailing address, in association with an individual's name.

More than 50% of RROSH decisions also involved identity and financial information. Employment information is involved in 27% of RROSH decisions.

In recent years, email addresses have been increasingly involved in RROSH breaches, while the prevalence of medical information has decreased. The increase in the percentage of breaches that involved transaction information, such as purchase history, reflects the increase in breaches caused by compromised electronic information systems, especially e-commerce websites.

TABLE 10: RROSH – Categories of Personal Information – Percent of Decisions as Yearly Total

Note: Each decision may include more than one category of personal information.

CATEGORIES OF PERSONAL INFORMATION	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
Contact Information	75%	67%	73%	69%	81%	73%	76%	75%	74%	74%	87%
Identity	65%	76%	70%	65%	66%	56%	49%	46%	50%	45%	55%
Financial	60%	54%	40%	30%	44%	64%	62%	66%	49%	54%	56%
Employment	30%	30%	38%	24%	23%	22%	23%	17%	23%	20%	27%
Email Address	5%	20%	18%	22%	21%	34%	36%	32%	35%	40%	40%
Medical Information	35%	13%	8%	6%	14%	18%	15%	10%	14%	18%	12%
Credentials	0%	0%	0%	24%	36%	3%	1%	0%	0%	0%	0%
Insurance	0%	0%	0%	0%	0%	0%	0%	1%	1%	1%	0%
Transaction Information	0%	0%	3%	0%	3%	2%	4%	10%	6%	6%	5%

Harm

By definition, all RROSH breaches present a real risk of significant harm.

The types of harm arising from breach reports largely reflect the evolving causes of breaches and the personal information at issue in these breaches. Identity theft, fraud and risk of financial loss have been constants. More recently, phishing as a harm has been increasing, as more reported breaches involved stolen or compromised email addresses.

TABLE 11: RROSH – Type of Harm – Number of Decisions by Year

Note: Each decision may include more than one type of harm.

TYPE OF HARM	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
Identity Theft	29	58	59	71	111	111	121	170	211	218	250
Fraud	22	15	53	73	111	110	118	170	210	220	246
Financial Loss	3	1	5	15	20	36	41	70	47	28	58
Humiliation	4	8	13	13	34	36	39	46	82	92	77
Hurt	0	6	10	11	29	34	37	42	71	84	74
Phishing	0	12	9	15	17	43	48	75	89	120	166
Embarrassment	6	1	2	5	16	30	35	44	79	85	77
Damage to Reputation	2	7	8	4	9	13	23	17	18	21	18
Negative Effect on Credit Record	1	0	1	3	5	6	6	20	9	2	8
Access to or Compromise of Online Accounts	0	1	0	0	0	11	9	7	14	18	21
Damage to Relationships	0	1	4	5	5	0	3	1	9	13	11
Anxiety / Distress	3	0	0	0	0	0	0	0	0	1	6
Unsolicited Communication	0	0	0	1	0	1	3	3	4	1	0
Other Type of Harm	1	2	2	0	6	7	4	5	6	7	6
No Harm	16	23	11	8	4	8	8	16	12	10	12
Unknown	0	0	3	2	0	0	1	1	2	0	0

Likelihood of Significant Harm

The likelihood of significant harm increases when there is deliberate action or malicious intent (that is, the breach is not accidental). These breaches usually result in RROSH decisions. Ransomware attacks, system hacks, theft, phishing and deliberate action by rogue employees are all examples of deliberate action or malicious intent to cause the breach. The majority of RROSH breaches for which there was no deliberate action are unauthorized disclosures of personal information.

TABLE 12: RROSH – Deliberate Action or Malicious Intent – Percent of Decisions as Yearly Total

DELIBERATE ACTION OR MALICIOUS INTENT	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL %
Yes	60%	59%	55%	70%	53%	78%	73%	73%	69%	68%	80%	**71%**
No	30%	37%	43%	28%	44%	19%	24%	27%	27%	29%	20%	**27%**
Possible	10%	4%	3%	2%	2%	3%	2%	1%	5%	3%	0%	**2%**

Another factor that contributes to a RROSH decision is whether the personal information at issue in a breach is recovered or returned. This is seldom the case for a breach involving a compromised electronic information system in which personal information is accessed and exfiltrated. These types of breaches also increase the possibility that the personal information is disclosed further, by selling or posting the information on the dark web or in some other public forum, for example.

Similarly, the length of time that the personal information is exposed is often a factor in making a RROSH decision. The longer it takes for organizations to detect breaches (and, in particular, compromised electronic information systems) the greater the likelihood that a breach will result in a RROSH decision.

Number of Notifications to Affected Individuals[11]

Section 19 of the PIPA Regulation says:

> 19 A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information:
>
> ...
>
> (e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

Of the 1,334 RROSH decisions issued during the period, 1,062 included information about the total number of notifications to affected individuals. In 272 decisions, the reporting organization did not provide or was not able to confirm the overall number of affected individuals.

11 If a range was provided by the organization, the higher number was used. If no number was provided, and decision was RROSH, the number of individuals whose information was collected, used or disclosed in Alberta was used.

TABLE 13: RROSH – Number Range of Affected Individuals – Number of Decisions by Year

NUMBER OF AFFECTED INDIVIDUALS	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
1	2	4	4	3	9	9	12	18	23	34	31
2 - 10	2	6	2	11	19	9	9	18	33	35	19
11 - 100	9	10	9	9	19	19	15	23	46	28	43
101 - 1,000	4	12	8	12	17	16	19	23	31	38	57
1,001 - 100,000	2	7	10	7	12	21	16	22	30	38	66
100,000 or more	0	6	1	1	2	6	6	4	7	8	11
Unknown	1	1	6	11	8	11	21	58	50	50	55

TABLE 14: RROSH – Number of Notifications

NUMBER OF NOTIFICATIONS	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
Actual Total Number (in 1000s)*[12]	6	137,193	610	268	11,808	38,759	3,101,447	3,359	521,686	57,656	41,272
Average Number (in 1000s)	-	3,049	18	6	151	484	40,279	31	3,069	319	182

*Since a given individual may have been affected by more than a privacy breach in a given year, these totals should not be considered to represent unique individuals.

12 Real values: 6,221; 137,192,839; ,609,723; 267,566; 11,807,921; 38,759,196; 3,101,446,722; 3,359,205; 521,685,562; 57,655,860; 41,272,002

Number of Affected Individuals in Alberta

Of the 1,334 RROSH decisions issued during the period, 1,244 included information about the total number of affected individuals whose personal information was collected, used or disclosed in Alberta. In 90 decisions, the reporting organization did not provide or was not able to confirm the exact number of affected individuals whose information was collected, used or disclosed in Alberta.[13]

TABLE 15: RROSH – Number Range of Affected Individuals – Number of Decisions by Year

NUMBER OF AFFECTED INDIVIDUALS	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
1	3	5	4	9	10	14	16	32	40	53	47
2 - 10	3	8	3	9	24	20	20	39	62	61	64
11 - 100	10	10	11	16	20	25	26	41	57	50	69
101 - 1,000	4	9	8	9	19	18	20	25	23	29	53
1,001 - 100,000	0	9	5	3	7	6	13	18	13	22	38
100,000 or more	0	2	1	1	1	1	1	0	1	2	2
Unknown	0	3	8	7	5	7	1	10	3	1	7
N/A	0	0	0	0	0	0	1	1	21	13	2

13 The number of affected individuals is based on what organizations report, and there is often no distinction made between Alberta residents and individuals whose information was collected, used or disclosed in Alberta.

TABLE 16: RROSH – Number of Notifications

NUMBER OF NOTIFICATIONS	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021
Total Number (in 1000s)*[14]	2	1,021	263	765	357	315	949	217	1,858	571	1,951
Average Number (in 1000s)	-	24	8	16	4	4	10	1	9	3	7

*Since an individual may have been affected by more than one privacy breach in a given year, these totals should not be considered to represent unique individuals.

There is no discernable trend year to year regarding the number of notices to affected individuals. In 2010-2011, 1,821 notifications were required as a result of breaches under PIPA, and in 2020-2021, 1,951,180 notifications were required.

Notifying Affected Individuals

Section 37.1(1) of PIPA says:

> Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, **the Commissioner may require the organization to notify individuals** to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure [emphasis added]

Section 37.1(7) says, "Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information."

In 2010-2011, organizations had notified affected individuals in approximately 55% of breaches reported to the OIPC. Since 2012-2013, at least 80% of organizations had already notified affected individuals at the time the breach was reported to the Commissioner. In 2014-2015, 100% of organizations reporting breaches had already notified affected individuals, or indicated they intended to.

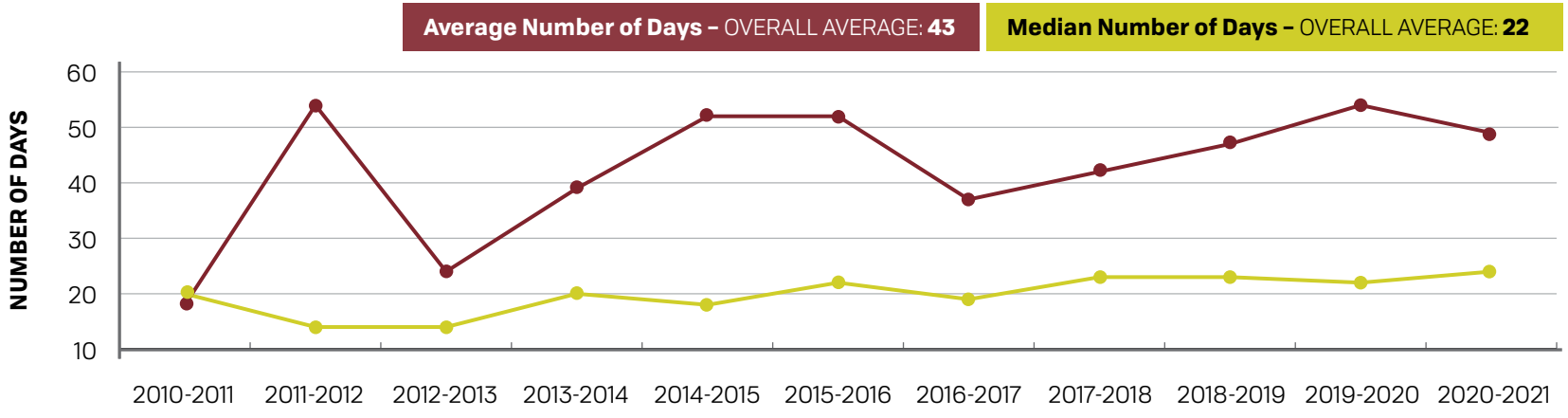
14 Real values: 1,821; 1,020,971; 263,133; 764,782; 357,328; 314,981; 948,522; 216,604; 1,857,971;570,745; 1,951,180.

Timelines – Days to Notify

Of the 1,334 RROSH decisions issued, 1,190 included enough information to compute the number of days that elapsed between the date the breach was discovered and the date the organization notified affected individuals. In 138 decisions, the date of discovery, the date of notice to the affected individuals, or both, were unknown or unreported.

TABLE 17 and FIGURE 5: RROSH – Number Range of Days to Notify – Number of Decisions by Year

DAYS TO NOTIFY	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
7 or less	3	11	10	8	23	23	29	39	54	75	77	**352**	**26%**
7 - 14	1	7	9	9	5	9	9	24	22	24	32	**151**	**11%**
14 - 30	2	3	9	7	15	18	22	29	36	38	53	**232**	**17%**
30 - 60	3	6	3	10	9	13	14	24	32	37	53	**204**	**15%**
60 or more	0	8	3	4	13	19	14	31	44	54	61	**251**	**19%**
Unknown	11	11	6	16	21	9	10	19	32	3	6	**144**	**11%**
Total	**20**	**46**	**40**	**54**	**86**	**91**	**98**	**166**	**220**	**231**	**282**	**1334**	



There are no discernable trends. Values varied significantly from year to year, with averages between 18 days and 54 days. Nonetheless, some observations can be made:

- Given the relatively small number of values in each fiscal year, any breach where the organization takes unusually long to notify affected individuals can significantly affect the average in a year.
- Breaches that involve "loss" and "unauthorized disclosure" have similar averages (37 and 39 days), while breaches involving "unauthorized access" have a higher average (55 days), and this is particularly the case from 2018-2019 to 2020-2021. The difference correlates to compromised electronic information systems often being difficult to discover and investigate.

Type of Notification

Section 19.1(1) of the PIPA Regulation requires organizations to notify affected individuals directly; however, notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances. Section 19.1 reads as follows:

> 19.1(1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must
>
> (a) be given directly to the individual, ...
>
> (2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

TABLE 18: RROSH – Type of Notification – Number of Decisions by Year

Note: Each decision may include more than one type of notification.

TYPE OF NOTIFICATION	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL %
Direct	17	41	36	48	85	88	94	159	204	227	275	**91%**
Indirect	0	0	2	0	0	0	0	1	1	2	2	**1%**
Both	0	2	2	0	1	6	2	6	8	7	18	**4%**
Unknown[15]	3	5	2	6	1	3	4	6	15	2	5	**4%**

15 Includes organizations for which details about notification type were not available and organizations that had not notified yet at the time they submitted their report to the OIPC.

In almost all RROSH decisions, organizations notified affected individuals directly, including by in-person meetings, telephone, mail or email. In some cases, organizations also notify individuals indirectly, such as a website posting, or by using social media or traditional media.

In 60 cases, the Commissioner authorized indirect notification. In 52 of those cases, the organization also notified some individuals directly. Indirect notification most commonly occurred when the organization did not have current contact information for all or some of the affected individuals.

Method of Notification

Most individuals are notified by mail, with an increasing number of people being notified by email and telephone.[16]

TABLE 19: RROSH – Method of Notification – Number of Decisions by Year

Note: Each decision may include more than one method of notification.

METHOD OF NOTIFICATION	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	% OF TOTAL
Email	2	13	8	11	14	40	34	50	72	89	141	**27%**
In Person	4	1	1	2	1	4	6	7	14	8	3	**3%**
Letter	10	18	26	38	42	50	57	104	125	134	159	**44%**
Published Notice	0	2	4	0	1	9	2	11	11	9	18	**4%**
Telephone	5	6	5	6	14	11	18	24	28	31	38	**11%**
Verbal	2	3	2	1	1	1	2	10	13	21	16	**4%**
Unknown[17]	5	15	2	8	26	6	9	8	18	6	9	**6%**

The increase in notification electronically suggests organizations are choosing this method because of the increased use of email between individuals and organizations, the speed of delivery, or cost. It may also be that organizations only have email addresses of customers and no other contact information. PIPA and the PIPA Regulation do not specify the method of notification.

16 The OIPC's dataset does not include method of notification for 2010-2011 and 2011-2012.

17 Same as footnote 16.

A "Typical" RROSH Breach in 2010 and 2021[18]

2010: The breach was a loss of personal information of employees, with some customers affected. The personal information was stolen and not recovered. Theft indicates there was deliberate action or malicious intent involved. The personal information involved was primarily contact, identity and financial information, and some medical information. The personal information at issue could be used to cause the significant harms of identity theft and fraud. The organization discovered the breach in 18 days. After discovering the breach, it took the organization 18 additional days to notify affected individuals and 26 additional days to report the breach to the OIPC. There were 311 individuals affected, of whom 91 had their personal information collected, used or disclosed in Alberta. The organization notified affected individuals directly, by letter.

2021: The breach was an unauthorized access to personal information of customers, with some employees affected. The unauthorized access of personal information occurred through a compromised electronic information system, likely due to social engineering or phishing. A compromised electronic information system indicates there was deliberate action or malicious intent involved. The personal information involved was contact, financial and identity information, and some email addresses. The personal information at issue could be used to cause the significant harms of fraud, identity theft and phishing. The organization discovered the breach in 57 days. After discovering the breach, it took the organization 49 additional days to notify affected individuals and 60 additional days to report the breach to the OIPC. There were 146,355 individuals affected, of whom 6,919 had their personal information collected, used or disclosed in Alberta. The organization notified affected individuals directly, by letter or email.

18 Hypothetical scenarios that depict the average characteristics of RROSH breaches in 2010-2011 and 2020-2021.

NO RROSH DECISIONS

This section focuses on the characteristics of breach reports that were determined to be no real risk of significant harm (NO RROSH) to affected individuals.

Of the 1,953 decisions issued, 21% (or 419) were determined to be NO RROSH.

Although the actual number of NO RROSH breaches increased overall, there has been a relative decrease in the number of NO RROSH decisions as a percentage of yearly total.

TABLE 20: NO RROSH – Number of Decisions Issued

NUMBER OF DECISIONS	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
NO RROSH	22	28	31	26	34	38	47	56	44	55	38	**419**
Annual % Change	-	27%	11%	-16%	31%	12%	24%	19%	-21%	25%	-31%	
% of Yearly Total	44%	30%	37%	27%	25%	26%	29%	24%	15%	18%	11%	

Of the 419 decisions issued, 78% (326) involved unauthorized disclosure of personal information, 13% involved a loss of personal information (53), and 9% involved unauthorized access to personal information (39). The primary cause of breaches that resulted in a NO RROSH decision has been transmission errors.

TABLE 21: NO RROSH – Type of Breach – Number of Decisions by Year and Percent of Decisions as Yearly Total

TYPE OF BREACH	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL
Loss	6	6	2	5	1	5	9	3	6	8	2	**53**
% of Yearly Total	27%	21%	6%	19%	3%	13%	19%	5%	14%	15%	5%	**13%**
Unauthorized Access	2	6	4	4	3	0	4	6	4	3	3	**39**
% of Yearly Total	9%	21%	13%	15%	9%	0%	9%	11%	9%	5%	8%	**9%**
Unauthorized Disclosure	14	16	25	17	29	33	34	47	34	44	33	**326**
% of Yearly Total	64%	57%	81%	65%	85%	87%	72%	84%	77%	80%	87%	**78%**
Other	0	0	0	0	1	0	0	0	0	0	0	**1**
% of Yearly Total	0%	0%	0%	0%	3%	0%	0%	0%	0%	0%	0%	**0%**
Decisions Total	**22**	**28**	**31**	**26**	**34**	**38**	**47**	**56**	**44**	**55**	**38**	**419**

Most NO RROSH breaches are accidental. Errant email is the leading cause of NO RROSH breaches, followed closely by mailing errors. Most commonly, these errors result when an individual's personal information is sent to an incorrect recipient, or the correct recipient receives their personal information but also that of another individual.

TABLE 22: NO RROSH – Breach Cause – Percent of Decisions as Yearly Total

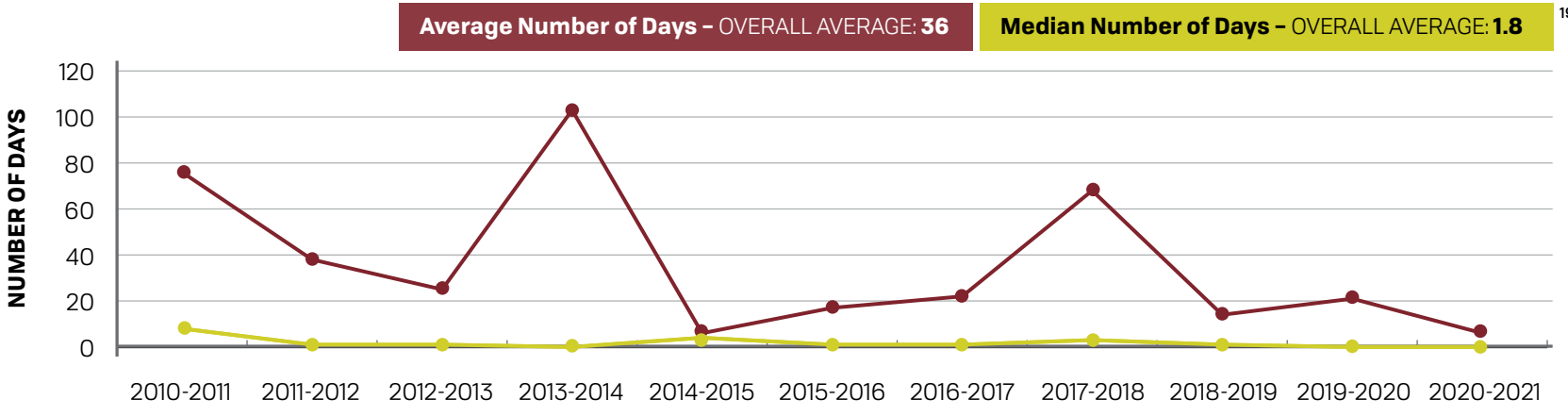
BREACH CAUSE	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	% OF TOTAL
Theft	14%	11%	3%	15%	6%	13%	6%	0%	5%	5%	0%	**6%**
Transmission Errors	45%	43%	55%	46%	79%	63%	64%	68%	59%	60%	82%	**62%**
Compromised Electronic Information System	0%	11%	16%	12%	3%	0%	11%	11%	14%	9%	8%	**9%**
Misplaced or Lost Information	5%	11%	3%	8%	0%	0%	2%	0%	2%	4%	0%	**3%**
Failure to Secure	9%	11%	16%	4%	3%	13%	2%	13%	14%	22%	8%	**11%**
Other	27%	14%	6%	15%	9%	11%	15%	9%	7%	0%	3%	**9%**

Timelines – Days to Discover

Overall, NO RROSH breaches are detected relatively quickly, with 68% of NO RROSH breaches discovered in 7 days or less. Since most NO RROSH breaches are caused by transmission errors, the sender, recipient or both tend to quickly discover them.

TABLE 23 and FIGURE 6: NO RROSH – Days to Discover – Number of Decisions by Year

DAYS TO DISCOVER	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
7 or less	10	22	17	10	24	30	36	32	31	42	31	**285**	**68%**
7 - 14	2	1	3	1	4	1	4	6	4	2	2	**30**	**7%**
14 - 30	3	1	0	0	1	3	1	4	4	5	1	**23**	**5%**
30 - 60	0	0	2	1	1	0	0	1	1	1	0	**7**	**2%**
60 or more	6	3	3	2	0	3	4	7	3	3	2	**36**	**9%**
Unknown	1	1	6	12	4	1	2	6	1	2	2	**38**	**9%**
Total	**22**	**28**	**31**	**26**	**34**	**38**	**47**	**56**	**44**	**55**	**38**	**419**	**100%**



19 Values of '0' are due to most breaches in that fiscal year being discovered on the day they happened.

Industry Reporting

The dataset for NO RROSH breaches is smaller than for RROSH breaches. As a result, it is more difficult to draw conclusions based on the distribution of cases across industry categories.

As a general observation, however, of breaches reported in 2010-2011, more than 50% determined to be NO RROSH were spread across three industries:

Finance
23%

Health Care and Social Assistance
14%

Insurance
14%

TABLE 24: NO RROSH – Industry of Reporting Organization – Number of Decisions by Year and Percent as Yearly Total

INDUSTRY	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL (%)
Accommodation and Food Services	1 (5%)	0 (0%)	1 (3%)	0 (0%)	1 (3%)	0 (0%)	1 (2%)	1 (2%)	0 (0%)	0 (0%)	1 (3%)	**6 (1%)**
Administrative and Support and Waste Management and Remediation Services	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	**2 (0%)**
Agriculture, Forestry, Fishing and Hunting	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	**0 (0%)**
Arts, Entertainment, and Recreation	0 (0%)	0 (0%)	1 (3%)	1 (4%)	0 (0%)	0 (0%)	2 (4%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	**5 (1%)**
Construction	0 (0%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	1 (3%)	0 (0%)	0 (0%)	1 (2%)	2 (4%)	0 (0%)	**5 (1%)**
Educational Services	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (5%)	2 (4%)	0 (0%)	2 (5%)	1 (2%)	0 (0%)	**7 (2%)**
Finance	5 (23%)	5 (18%)	5 (16%)	6 (23%)	15 (44%)	15 (39%)	12 (26%)	21 (38%)	8 (18%)	15 (27%)	10 (26%)	**117 (28%)**
Insurance	3 (14%)	3 (11%)	6 (19%)	8 (31%)	7 (21%)	4 (11%)	4 (9%)	8 (14%)	4 (9%)	3 (5%)	1 (3%)	**51 (12%)**
Health Care and Social Assistance	3 (14%)	1 (4%)	1 (3%)	0 (0%)	3 (9%)	6 (16%)	4 (9%)	2 (4%)	7 (16%)	10 (18%)	8 (21%)	**45 (11%)**
Information	0 (0%)	1 (4%)	0 (0%)	1 (4%)	1 (3%)	0 (0%)	0 (0%)	2 (4%)	2 (5%)	0 (0%)	2 (5%)	**9 (2%)**
Manufacturing	1 (5%)	3 (11%)	0 (0%)	1 (4%)	2 (6%)	0 (0%)	1 (2%)	4 (7%)	3 (7%)	1 (2%)	2 (5%)	**18 (4%)**

INDUSTRY	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL (%)
Mining, Quarrying, and Oil and Gas Extraction	1 (5%)	1 (4%)	1 (3%)	3 (12%)	0 (0%)	5 (13%)	4 (9%)	1 (2%)	0 (0%)	1 (2%)	0 (0%)	**17 (4%)**
Other Services (except Public Administration)	2 (9%)	7 (25%)	5 (16%)	3 (12%)	2 (6%)	3 (8%)	5 (11%)	6 (11%)	3 (7%)	8 (15%)	4 (11%)	**48 (11%)**
Professional, Scientific, and Technical Services	2 (9%)	2 (7%)	5 (16%)	1 (4%)	1 (3%)	2 (5%)	5 (11%)	4 (7%)	6 (14%)	4 (7%)	5 (13%)	**37 (9%)**
Public Administration	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	**0 (0%)**
Real Estate and Rental and Leasing	1 (5%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (4%)	2 (4%)	1 (2%)	1 (2%)	2 (5%)	**10 (2%)**
Retail Trade	2 (9%)	1 (4%)	3 (10%)	2 (8%)	1 (3%)	0 (0%)	3 (6%)	3 (5%)	6 (14%)	5 (9%)	2 (5%)	**28 (7%)**
Transportation and Warehousing	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	**2 (0%)**
Utilities	0 (0%)	2 (7%)	2 (6%)	0 (0%)	1 (3%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	2 (4%)	1 (3%)	**8 (2%)**
Wholesale Trade	1 (5%)	0 (0%)	1 (3%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	0 (0%)	0 (0%)	**3 (1%)**
Unknown	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	1 (2%)	0 (0%)	0 (0%)	**1 (0%)**

In 2020-2021, the top industry sectors reporting breaches were:

- Finance (26%)
- Health Care and Social Assistance (21%)
- Professional, Scientific, and Technical Services (13%)
- Other Services (except Public Administration) (11%)

Overall, the distribution across industries presents many similarities with that of RROSH breaches. The finance sector was most prevalent most years and the insurance sector was most prevalent in 2012-2013 and 2013-2014. These two industry sectors account for the majority of NO RROSH breaches. Organizations in these industries report a large number of breaches to the OIPC every year, even when the RROSH threshold is not met. It may be because these are highly regulated industries.

Since they are mostly due to human error – and overwhelmingly, transmission errors – NO RROSH breaches are primarily associated with organizations in industries that routinely send information to individuals, such as the Finance and Insurance industries."

Notifying Affected Individuals

Organizations are not required to notify affected individuals where there is no real risk of significant harm as a result of the breach. Nonetheless, for the majority of NO RROSH breaches, organizations had already notified affected individuals at the time of reporting the breach to the Commissioner. Of the 419 NO RROSH decisions issued, 290 of the corresponding breach reports indicated that the organization had notified individuals. In all but one case, these organizations notified affected individuals directly.

A "Typical" NO RROSH Breach – 2010 vs. 2021[20]

2010: The breach was an unauthorized disclosure of personal information. The personal information was accidentally mailed to an unintended recipient. The organization confirmed that the unintended recipient destroyed the personal information. The organization discovered the breach in less than 7 days. Despite no requirement to do so, the organization notified affected individuals.

2021 The breach was an unauthorized disclosure of personal information. The personal information was accidentally emailed to unintended recipients. The organization confirmed that the unintended recipients destroyed the personal information. The organization discovered the breach in less than 7 days. Despite no requirement to do so, the organization notified affected individuals.

20 Hypothetical scenarios that depict the average characteristics of NO RROSH breaches in 2010-2011 and 2020-2021.

NO JURISDICTION FINDINGS

This section focuses on the characteristics of breach reports that were determined to be No Jurisdiction.

Of the 1,953 decisions issued, 200 (or 10%) were determined to be No Jurisdiction.

The number of No Jurisdiction breaches as a percentage of yearly total peaked in 2011-2012 (21% of breaches reported) and has been declining since 2013-2014.

TABLE 25: No Jurisdiction – Reasons for Decision – Number of Decisions by Year

REASONS FOR DECISION	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	TOTAL	% OF TOTAL
No Collection, Use or Disclosure in Alberta	0	0	1	4	8	8	6	3	4	1	6	**41**	**21%**
No Breach	0	2	5	4	1	0	1	4	7	5	6	**35**	**18%**
Federal Work, Undertaking or Business	4	1	0	0	1	0	1	3	8	6	8	**32**	**16%**
Non-Profit	1	4	3	0	1	4	3	2	2	3	9	**32**	**16%**
Organization Does Not Have Control	0	5	1	3	3	5	4	2	0	0	4	**27**	**14%**
PIPA Does Not Apply	2	4	1	3	1	0	3	0	1	2	0	**17**	**9%**
Not Personal Information	0	1	0	0	1	0	1	0	3	2	0	**8**	**4%**
Not an Organization	1	2	0	0	1	0	0	0	0	1	0	**5**	**3%**
Incomplete	0	1	1	1	0	0	0	0	0	0	0	**3**	**2%**
Total	**8**	**18**	**6**	**7**	**8**	**9**	**12**	**7**	**14**	**14**	**21**	**200**	**100%**

Collection, Use or Disclosure within Alberta

The most common reason for a No Jurisdiction decision is when personal information is not collected, used or disclosed in Alberta, representing 21% of No Jurisdiction decisions. PIPA will apply when an organization collects, uses or discloses personal information within Alberta.

No Breach

Section 34.1 of PIPA requires organizations to provide notice to the Commissioner "of any incident involving the loss of or unauthorized access to or disclosure of the personal information."

In 18% of No Jurisdiction decisions issued, the OIPC determined that the incident was not a breach (that is, there was no loss of or unauthorized access to or disclosure of personal information).

Federal Work, Undertaking or Business

An organization that is a "federal work, undertaking or business" that collects, uses and discloses personal information in Alberta is subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Office of the Privacy Commissioner of Canada is responsible to ensure compliance with PIPEDA.

In most cases, breach reports received by the OIPC that are determined to fall under PIPEDA relate to airlines, telecommunications companies or banks.

An organization other than a "federal work, undertaking or business" collecting, using or disclosing personal information in Alberta is exempt from the application of PIPEDA.[21]

Non-Profit

Under section 56(1) of PIPA, "non-profit organization" is defined to mean an organization that is incorporated under Alberta's *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*.

Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity.

Of the 200 No Jurisdiction decisions issued, 16% were because the reporting organization was a "non-profit organization" as defined in PIPA and the personal information at issue was not collected, used or disclosed in connection with any commercial activity.

Organization Does Not Have Control

Section 34.1(1) of PIPA requires "[a]n organization having personal information under its control..." to provide notice to the Commissioner of certain breaches.

Having custody of personal information involved in a reportable breach does not necessarily trigger the reporting requirements of section 34.1. For example, if an organization provides services to another organization, the service provider could have custody of the personal information but may not have personal information "under its control". The organization that "controls" the personal information is required to report the breach.

In some cases, a No Jurisdiction decision will be issued when an organization that does not have control of personal information reports a breach.

21 Pursuant to the Organizations in the Province of Alberta Exemption Order, SOR/2004-219.

PIPA Does Not Apply

In some cases, breaches are reported to the OIPC under section 34.1 of PIPA, but after clarifying with the reporting organization, it was determined that either Alberta's *Freedom of Information and Protection of Privacy Act or Health Information Act* applied.

On rare occasions, breaches were reported in relation to personal information under the control of entities operating in Alberta but that do not fall under provincial privacy legislation, such as political parties.

PIPA did not apply in 9% of No Jurisdiction decisions.

Not Personal Information

Section 1(1)(k) of PIPA defines "personal information" to mean "information about an identifiable individual".

In 8 No Jurisdiction decisions issued, the OIPC found that the information at issue was not personal information as defined in PIPA. Most commonly, these breaches involved corporate credit cards or other corporate information.

Not an Organization

PIPA applies to "organizations", defined in section 1(1)(i) of the Act as follows:

> (i) "organization" includes
>
> (i) a corporation,
>
> (ii) an unincorporated association,
>
> (iii) a trade union as defined in the Labour Relations Code,
>
> (iv) a partnership as defined in the Partnership Act, and
>
> (v) an individual acting in a commercial capacity,
>
> but does not include an individual acting in a personal or domestic capacity;

Of 200 No Jurisdiction decisions issued, 5 found that the entity reporting the breach was not an organization as defined in PIPA. For example, the breach might have been reported by an individual acting in a personal capacity or the organization had ceased to exist due to bankruptcy. In such cases, there is no "organization" that the Commissioner can require to notify affected individuals.

APPENDIX A: BREACH REPORTING AND NOTIFICATION PROVISIONS

PIPA Provisions

Notification of loss or unauthorized access or disclosure

34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

...

Power to require notification

37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms or conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

...

59(1) Subject to subsections (3) and (4), a person commits an offence if the person...

(e.1) fails to provide notice to the Commissioner under section 34.1

PIPA Regulation Provisions

In April 2010, the Minister of Service Alberta issued an order in council that amended the *Personal Information Protection Act Regulation*, and included the information elements required when reporting a breach to the Commissioner or notifying affected individuals.[22] In addition to prescribing what information must be disclosed to affected individuals, provisions also noted that direct notice is required unless "the Commissioner determines that direct notice would be unreasonable in the circumstances."

The notice requirements read:

Part 6

Notification of Loss of or Unauthorized Access to or Disclosure of Personal Information

Notice to the Commissioner

19 A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information:

(a) a description of the circumstances of the loss or unauthorized access or disclosure;

22 Alberta Queen's Printer, O.C. 123/2010, A.R. 51/2010, April 15, 2010.

(b) the date on which or time period during which the loss or unauthorized access or disclosure occurred;

(c) a description of the personal information involved in the loss or unauthorized access or disclosure;

(d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;

(e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

(f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

(g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;

(h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

Notification to individuals

19.1(1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must

(a) be given directly to the individual, and

(b) include

(i) a description of the circumstances of the loss or unauthorized access or disclosure,

(ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,

(iii) a description of the personal information involved in the loss or unauthorized access or disclosure,

(iv) a description of any steps the organization has taken to reduce the risk of harm, and

(v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

(2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

Office of the Information and
Privacy Commissioner of Alberta