File Number	Respondent	Date Received	Date of Incident	Description
PA-051842	[redacted]	1/11/2018	12/20/2017	A third party gained access, likely through a phishing scam, to emails sent to a small group of [redacted] employees. The employees whose emails were accessed all work in Mississauga, ON, at [redacted] Support Office. This event involved a privacy breach for some former and current employees, as well as fourteen of our clients, all of whom reside in Ontario. Personal information involved: Clients—name and medical information. Employees and former employees—name, Social Insurance Number (for some individuals), financial information (for some individuals), health card number (for one individual). Number of affected individuals 127
PA-054340	Non-Public Property and Staff of the Non-Public Funds,	11/22/2018	11/14/2018	CFMWS was alerted on November 22 about a malicious attack that has potentially compromised 319 credit cards on the CANEX.ca website between November 14-21. The attack was code script placed into to the software that followed the user as they accessed the pages of CANEX.CA. It sent all the user inputted information (eg. their personal/credit card information) to the intended destination and a mirror copy to the hackers. This allows the external destination to use the information themselves or to sell the information on the black market. - Number of affected individuals 314
PA-055448	National Film Board of Canada	4/25/2019	2/9/2019	L'ONF s'est fait attaquer par un virus nommé Trickbot au courant de la semaine du 4 février 2019. Ce premier virus a été contrôlé par nos équipes, cependant, Trickbot s'est répandu. Il leur a pris quelques semaines pour s'assurer qu'il soit complètement disparu et nettoyé de nos dispositifs. Le Centre canadien de Cybersécurité à d'ailleurs été impliqué dans le processus de détection et de nettoyage. Type de renseignments personnels en cause: Mots de passe des utilisateurs de l'organisation qui étaient enregistrés dans leurs navigateurs. L'ONF affirme que dans ce cas-ci, une plainte est non-applicable considrant le fait que les informations personnelles qui ont été compromises n'ont pas été demandées par l'ONF à l'employé. D'ailleurs, tous les employés ont reçu une note les avisant des risques potentiels de compromission des mots de passe leur indiquant de: 1) changer leur mot de passe personnel; 2) ne pas enregistrer de mots de passe dans leurs navigateurs. Toutefois, l'ONF a contacté les partenaires du gouvernement canadien le 11 et 12 février pour les information de la situation. Number of affected individuals 3

s.16(1)(b)
s.16(1)(c)
s.16(2)(c)

File Number	Respondent	Date Received	Date of Incident	Description
PA-056557	Canada Post Corporation	10/16/2019	7/1/2019	On October 3, 2019, Canada Post received notification from [redacted] that credentials associated with approximately 4000 candapost.ca accounts were being sold in an online forum located on the dark web. These credentials are email addresses and passwords. The accounts were posted to the online forum in July and August 2017. On October 11, 2019, the Canada Post Security and Investigations Team [redacted] Through engaging a third party forensic team, it was further determined that the compromised credentials came from previous external data breaches that is, data breaches of third parties [redacted] In other words, the breach is not a result of a compromise of the Canada Post network/environment. Further investigation resulted in the determination that 107 canadapost.ca accounts out of the total number of the involved accounts were accessed by unauthorised users. Canada Post is in the process of notifying the affected account holders; and a forced password reset is being deployed across the network (both the 107 affected accounts and as a proactive safeguarding measure - all the accounts). At the same time, [redacted] canadapost.ca users are being reminded of the importance of not re-purposing their login credentials across different websites. Finally, Canada Post is offering free credit monitoring for one year to the 107 affected account holders. [redacted] Personal information involved: Information contained within payroll documents, utilities and property tax bills, as well as credit card statements. In most cases, the personal information is limited to the individuals' name, mailing address, the identity of the mailer (e.g., the employer, the financial institution, utilities service provider, etc.), and details such as the amount of a regular payment, balance on a credit card, etc. In the case of credit card statements, account numbers are masked. Canada Post does not have access to the actual documents / visibility into the contents. This is information belonging to individual mailers. 107 Affected Individuals
PA-058206	Transport Canada	8/17/2020	8/5/2020	On August 12, 2020, Transport Canada was informed of a cyber incident related to the GCKey where 24 departments were affected (including Transport Canada). The 9041 Government of Canada GCKey accounts were compromised by a cyber incident on August 5, 6, and 11, 2020. Transport Canada's Digital Services investigated and confirmed that the compromised GCKey credentials were not used to access TC's digital systems in almost all cases (5 exceptions). There may have been unauthorized access to five accounts linked to TC's General Aviation Licensing On-line (GALRO) system. No data was added or changed in the system for the five accounts. The probability and impact of the breach are both low. This breach is not material. Transport Canada is informing the Office of Privacy Commissioner given the scope of the cyber incident for the Government of Canada. Personal information involved: The type of personal information involved included pilot medical assessments and flight test / written test information. For the individuals' own files for personnel licensing, all five individuals have pilot licensing information. The overall personal information involved includes: Address, phone number, and email address; this information is editable, however, they were not updated in August 2020. Remaining pilot licensing information is read-only. This would include the expiry date of a license, medical information such as examination date and assessment, and score at a written test. Number of affected individuals 5
PA-058210	National Defence	8/18/2020	7/3/2020	On 03 July 2020, the Royal Military College (RMC) of Canada server was subject to a RANSOMWARE attack. On August 17th, National Defence, discovered that the active directory (user credentials) and list of host computers were ex-filtrated, which would affect all users of the RMC Network. Personal information involved: Secondary email accounts (personal emails), as well as files containing student records and financial data, may have also been compromised. Number of affected individuals 44

File Number	Respondent	Date Received	Date of Incident	Description
PA-058220	Employment and Social Development Canada	8/20/2020	8/5/2020	On August 5th, ESDC was informed by Shared Services Canada (SSC) of an active cyberattack on the GCKey credentials. Approximately 24 different federal departments and agencies use GCKey as a credential authority to access individual departmental accounts. The nature of the attack was a "credential stuffing attack" in which the threat agent used user names and passwords that are believed to have been acquired by the perpetrators from the dark web. These were used in an attempt to sign into GCKey. As part of this government wide attack, ESDC experienced approximately 8,100 attempts, of which 3,439 were successful in gaining access to My Service Canada (MSCA), Record of Employment (ROE) Web accounts, Grants and Contributions On-line Services (GCOS) and Canada Student Loan Program (CSLP) accounts. In mid-August, an additional 225 accounts were deemed to be subject to follow up attacks. On August 5th, ESDC was informed by Shared Services Canada (SSC) of an active cyberattack on the GCKey credentials. Approximately 24 different federal departments and agencies use GCKey as a credential authority to access individual departmental accounts. Number of affected individuals 12,320
PA-058270	International Development Research Centre	9/2/2020	7/3/2020	IDRC became aware of a cyber security incident that resulted in unauthorized access to its infrastructure on July 3. The incident was brought to its attention by the Canadian Centre for Cyber Security. Personal information involved: to be determined Number of affected individuals 1075
PA-058359	Royal Canadian Mounted Police	9/18/2020	7/1/2020	In July, the RCMP learned that a hacker group called Distributed Denial of Secrets had published over 260 gigabytes of law enforcement data it had stolen from the websites of 200+ law enforcement agencies. On 2020-07-07, the dataset was received by the RCMP and was analyzed. At this stage of analysis, the vast majority of the files relating to the RCMP are lists of event training registrations containing details of individuals signing up for various training events. Additional searches are ongoing. Personal information involved: Of the information identified as belonging to RCMP to date, the personal information involved includes employee names, home addresses, personal phone numbers, partial credit card numbers (including CVN and expiry dates) and dates of birth. - Number of affected individuals 123
PA-058396	Canada Revenue Agency	9/25/2020	7/10/2020	Information was compromised through credential stuffing attacks on two different paths: 1) GCKey and 2) CRA Credential Management System/Authentication Management System. The details about this breach are as of September 17, 2020, and as the investigation is still ongoing they are subject to change. Personal information involved: Tax, financial and personal information (addresses, telephone numbers, bank accounts) as well as relationships (representative authorizations) Number of Affected Individuals 48,500
PA-058397	Royal Canadian Mounted Police	9/25/2020	6/1/2020	A total of 97 GCKey accounts linked to RCMP services were affected as a result of this attack (73 Canadian Anti-Fraud Centre clients, 24 Canadian Firearms Program clients) however, there is no indication that any individual's personal information was materially affected. - Number of Affected individuals 97
PA-058672	Non-Public Property and Staff of the Non-Public Funds,	11/5/2020	7/3/2020	On 03 July 2020, the Canadian Defence Academy experienced a cyber ransomware attack that affected their entire network, including the Royal Military College of Canada (RMC) and three institutions in Ontario and Quebec. On 18 August 2020, Canadian Armed Forces (CAF) informed CFMWS that CFMWS-related member information may have been compromised as part of the incident. CFMWS was subsequently informed that 679 files had been dumped and potentially sold on the Dark Web as a result of the cyber ransomware attack. As some CFMWS PSP employees work on the RMC network, it is reasonable to assume that the threat actors may have accessed and infiltrated all of the PSP files saved on the RMC network even though at this point it has not all been exposed on the Dark Web. As of now, CFMWS still does not have confirmation from RMC how the data was compromised. PI: Name, contact information, biographical information, date of birth (DOB), educational information, employment information, employee identification number, other number or particular assigned to the individual (i.e. CFOne card #) Social Insurance Numbers (SIN) and financial information. - Number of Affected individuals 163

s.16(1)(c)
s.16(2)(c)

File Number	Respondent	Date Received	Date of Incident	Description
PA-059199	Canada Revenue Agency	1/22/2021	11/25/2020	[redacted]
PA-059272	Canada Coucil for the Arts	2/12/2021	9/1/2020	The Canada Council for the Arts (the "Council") has experienced an email compromise attack that has resulted in a breach of its Office 365 environment. The attack was detected on January 29, 2021, when a grant recipient requested an update on the status of a payment they had made to the Council. This resulted in the discovery that the payment had been intercepted by a third party that had gained access to and use of the Council's email systems. Following this, the Council engaged external digital forensics consultants to determine the nature, source and extent of the compromise and to secure our systems. The investigation to date indicates that the earliest evidence of the attack dates to September 2020. It is currently believed a Council employee clicked a phishing email link and responded to a request to enter their Council email account password. However, the root cause of the incident remains under investigation. The attack resulted in the attacker gaining access to the employee's account, and to the Council's Office 365 environment more broadly. We are working to determine the number of Council user accounts affected. At the time of writing we have identified two affected accounts. The attacker gained the ability to: •Access the environment, including viewing emails sent and received by the affected Council accounts, or sending email from the affected accounts, •Authorization to add further users to the system, •Use the newly added users to send email that would appear to the recipient to have come from the Council, for example, impersonating persons or roles within the Council, •Create forwarding rules to redirect email received by the Council. The attacker used this access to the system to send fraudulent email to recipients of grants from the Council, appearing to come from the Council, in an effort to convince the recipient to direct payments they were making to the Council via payment methods such as wire transfer or e-transfer to financial accounts of the attacker. Our grant recipients have reported four cases of such fraud attempts directed to them to date. Unfortunately, three of these attempts were successful, resulting in the theft of funds grant recipients were seeking to pay to the Council, by redirection of the transfer of funds to the attacker. The losses incurred in these cases were $44,000, $5,700, and $32,000. On February 5, 2021, the Council sent notice to its grant recipients informing them that fraudulent emails appearing to come from the Council had been detected, and were targeting grant recipients to obtain their financial information and redirect payments. The notice informed recipients that the Council would never request financial or banking information by email, that recipients should verify any transfers of funds, and provided them with Council contact information to report suspicious messages appearing to come from the Council. 10,732 individuals were notified of the incident

File Number	Respondent	Date Received	Date of Incident	Description
PA-059938	National Security and Intelligence Review Agency	5/20/2021	3/9/2021	NSIRA experienced a cyber incident linked to the successful exploitation of a set of Microsoft Exchange vulnerabilities between March 9 and March 19, 2021. The compromise affected NSIRA's externally-facing network, which houses information at the unclassified, Protected "A" and Protected "B" levels (the "Protected B network"). The compromise did not affect NSIRA's classified systems. Personal information involved: See details in breach report - Numer of affected individuals 129
PA-059968	Canada Post Corporation	5/25/2021	11/18/2020	On November 18th, 2020, Canada Post was made aware of a ransomware attack that impacted the operations of Commport, a supplier that offers electronic data interchange (EDI) solutions in support of Canada Post's parcel business. The manifest data of Canada Post's large commercial customers flows through Commport's network as part of the shipping process. Upon discovering the breach, an investigation was initiated by Commport and supported by a leading cyber security expert. No evidence was found that any data had been accessed, lost or stolen. On May 19th, 2021 Canada Post received notification by Commport that manifest data associated with some larger Canada Post commercial customers was found to be available for download on the dark web. On May 20th, 2021 Canada Post triggered its formal breach response process and engaged external cyber security experts to help manage the incident. Personal information involved: The impacted personal information is that of the end users/customers of Canada Post's commercial customers. The impacted personal information may include some or all information items as follows: oshipper number oshipper name ocustomer (consumer) first name, last name ocustomer (consumer) address ocustomer (consumer) email address ocustomer (consumer) phone number Number of Affected individuals 954, 375