OAIC – DATA BREACH NOTIFICATION [6 JANUARY 2023]

Part one - Statement about an eligible data breach

About part one

The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required). You must complete this section.

Organisation/agency details	
Organisation/agency name	Fire Rescue Victoria (ABN 28 598 558 561) (**FRV, we**)
Phone	1300 367 617
Email	frvassist@frv.vic.gov.au
Address Line 1	PO Box 151
Address Line 2	N/A
Suburb	East Melbourne
State	Vic
Postcode	3002
Other contact details	N/A

Description of the Eligible Data Breach	
A description of the eligible data breach *This needs to align with what was provided to individuals*	We were made aware of a cyber-attack on our internal IT environment on 15 December 2022. The incident affected a number of our internal servers (including our email system). We are working closely with cyber security experts and our partners in the State and Federal Governments, including the Australian Cyber Security Centre, to investigate and respond to this attack. While we continue to experience a widespread IT outage as a result of the attack, community safety has not been compromised and we continue to dispatch crews and appliances through mobile phones, pagers and radio. Our investigations about the cause and impact of this attack are ongoing. However, we have reasonable grounds to believe that personal information may have been accessed or stolen. Although we do not have evidence that personal information has been accessed or stolen from our systems, given the nature of the cyber-attack, we have reasonable grounds to believe that personal information of current and former employees, individual contractors and secondees of FRV and the former Metropolitan Fire and Emergency Services Board (as well as job applicants and other individuals) may have been accessed or stolen by a malicious third party.

Information Involved in the Data Breach	

Kind or kinds of personal information involved in the data breach	It is a complex task to identify what information is involved in this attack.
	
	While this analysis progresses, we are assuming that information that may have been accessed or stolen by a malicious third party includes personal information about:
	
	• current and former employees of FRV and the former Metropolitan Fire and Emergency Services Board (**MFB**), individual contractors and secondees from other organisations to FRV and the former MFB (**FRV Staff**); and
	• job applicants for FRV roles or former MFB roles (excluding firefighter recruit applicants).
	
	Based on our investigations to date, we have reasonable grounds to believe that the following personal information may have been accessed or stolen:
	
	A. Personal Information about current and former FRV Staff
	
	• Full Name
	• Address (current and previous)
	• Email address (current and previous)
	• Phone number (current and previous)
	• Date of birth
	• Health information
	• Sensitive information, to the extent any such information has been sent or received via our email system (for example, information about sexual orientation, race, disability, religion, qualifications, employment history, criminal history, political or religious views)
	• Bank account details (BSB, account name and number) (excluding secondees from other organisations and labour hire employees)
	• Superannuation details (excluding secondees from other organisations and labour hire employees)
	• Government issued identity information, to the extent any such information has been sent or received via our email system, such as:
	  ○ Driver's licence details
	  ○ Passport details
	  ○ Tax File numbers
	  ○ Birth, death and marriage certificates
	
	B. Personal Information about job applicants
	
	• Full Name
	• Address (current and previous)
	• Email address (current and previous)
	• Phone number (current and previous)
	• Date of birth
	• Sensitive information, to the extent any such information has been sent or received via our email system (for example, information about sexual orientation, race,

	disability, religion, qualifications, employment history, criminal history)
	• Government issued identity information, to the extent any such information has been sent or received via our email system, such as:
	  ○ Driver's licence details
	  ○ Passport details
	  ○ Tax File numbers
	
	As our email system has been affected by this attack, information that may have been accessed or stolen may also include personal information about other individuals (to the extent any such information has been sent or received by FRV Staff via our email system).

In addition, please select any categories that apply: ○ Financial Details ○ Tax File Number (TFN) ○ Identity Information (Centrelink Reference Number, Passport Number, Drivers Licence Number) ○ Contact Information (e.g. Home Address, Phone Number, Email Address) ○ Health Information ○ Other Sensitive Information (e.g. Sexual Orientation, Political or Religious Views)	Button Select • Financial Details • Tax File Number (TFN) • Identity Information (Passport Number, Drivers Licence Number) • Contact Information (e.g. Home Address, Phone Number, Email Address) • Health Information • Other Sensitive Information (e.g. Sexual Orientation, Political or Religious Views)

Recommended Steps	
Steps your organisation recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach	As there is a risk that personal information may have been accessed or stolen by a malicious third party, we strongly urge all current and former FRV Staff and job applicants to remain vigilant and take steps to protect their identity and credit profile. **TAKE ADDITIONAL CYBER SAFETY PRECAUTIONS** We recommend that all current and former FRV Staff and job applicants remain careful and vigilant with all online communications and transactions, and take the following steps: • Make sure you validate any communications you receive, to ensure they are legitimate • Be very careful when opening or responding to texts from unknown numbers and emails from unknown senders • Change account passwords (and replace with a strong password or passphrase – see latest Microsoft password

	advice) and enable multifactor authentication for banking and any other accounts where it is available • If you have reused your FRV password on personal accounts, you should go through these accounts and change the passwords • Do not click links in emails from unknown senders and check with known senders, before clicking links • Do not provide personal or credential information to people who contact you – legitimate organisations should not contact you and ask for this • Do not give remote access to your computer or mobile device • Learn to recognise scams and always be alert to phishing attempts (watch this video from the Australian Cyber Security Centre to learn how phishing scams work). **ADDITIONAL STEPS TO PROTECT YOUR IDENTITY** We have activated specialist monitoring services for all current and former FRV Staff and job applicants to use. If any current or former FRV Staff or job applicant is concerned about the potential misuse of their personal information, the individual can access free support from **IDCARE**, Australia's national identity and cybersecurity community support service. Each impacted individual can engage an IDCARE Case Manager via IDCARE's Get Help Web Form at www.idcare.org/contact/get-help using the **referral code FRV22**. We also urge all current and former FRV Staff and job applicants to follow specific identity protection advice: • Monitor all your devices and accounts for unusual activity. Go to scamwatch.gov.au for more information. Report unusual activity to Report Cyber at cyber.gov.au and IDCARE (1800 595 160, 8am-5pm Monday to Friday, excluding public holidays) • Monitor your bank accounts for any unusual or unauthorised activity and contact your financial institution immediately if you have any concerns. Ensure you have multifactor authentication in place, if available. • If you suspect fraud, you can request a ban on your credit report which 'freezes' access to your credit file (see guidance from IDCARE) • If you are the target or victim of a scam or believe your accounts have been compromised, lodge an online report via the Australian Cyber Security Centre (ACSC) • If you think someone has stolen your identity, contact IDCARE on 1800 595 160 (8am-5pm Monday to Friday, excluding public holidays). They have published several factsheets with advice specific to recent high profile Australian cyber breaches. **ADDITIONAL STEPS TO PROTECT YOUR CREDIT PROFILE** We have also partnered with Equifax, a leading provider of credit and identity monitoring services, to provide Equifax Protect to current and former FRV Staff and job applicants. Equifax Protect

	is a credit monitoring and identity protection service that helps reduce the risk of identity theft or financial loss. All current and former FRV Staff and job applicants are eligible for a 12-month Equifax Protect subscription, which includes: • monitoring of your personal information on the internet • alerts for changes on your credit reporting • monthly credit reports and score tracking. To activate Equifax Protect, each individual must follow the Equifax Protect registration instructions accessible on the FRV website. The individual will need to firstly request a personalised code. This is explained in the instructions. **ADDITIONAL SUPPORT AVAILABLE TO CURRENT FRV EMPLOYEES, RETIREES AND FAMILIES** Additional support is also available to current FRV employees, FRV retirees (including MFB retirees) and their families via our Employee Assistance Program (**EAP**). EAP provides access to external psychologists, social workers and counsellors. Should current FRV employees, retirees or their families require EAP support to help them manage their wellbeing during this time, FRV encourages them to reach out to FRV's Health and Wellbeing services. These services can be accessed by calling **1800 161 415**. **ADDITIONAL STEPS** As our email system has been affected by this attack, we strongly urge FRV Staff to contact us at frvassist@frv.vic.gov.au for further advice and assistance if they have any concern about the personal information of other individuals (for example, family members of FRV Staff) that may have been sent or received using our email system.

Other Entities Affected *If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.*	
Was another organisation affected? ○ Yes ○ No	Button select • No
Organisation Name	N/A
Phone	N/A
Email	N/A
Address Line 1	N/A

Address Line 2	N/A
Suburb	N/A
State	N/A
Postcode	N/A
Other Contact Details	N/A