



Facial Recognition Technology

Privacy Impact Assessment

May 2026

Contents

1. Project Introduction.....	4
1.1. Purpose of this PIA	4
1.2. Preparation of the PIA	4
2. FRT Overview.....	4
2.1. Background and reasons for using FRT	4
2.2. Methods attempted to address the problem	5
2.3. Proportionality Assessment.....	6
2.4. Review and Consultation Process.....	6
3. Use of the FRT System.....	7
3.1. The FRT System	7
Accuracy	7
3.2. How the FRT System Collects and Uses Personal Information	7
FRT System Personal Information Collection	7
Watchlist.....	8
3.3. The Types of Personal Information Collected	9
3.4. The Process if there is an Alert that there is a Match	9
3.5. Storage of Personal Information Collected by the FRT System.....	10
3.6. Access to the FRT System.....	10
3.7. Retention of Personal Information	10
3.8. Access to and Correction of Personal Information by an Individual	11
3.9. Disclosure of Personal Information	11
4. Compliance with the Information Privacy Principles	11
Privacy Principles under the Privacy Act 2020	11
Code Rules under the Biometric Processing Privacy Code 2025.....	11
Principle 1 – Purpose of the collection of personal information	12
Rule 1 - Purpose of the collection of biometric information	12
Principle / Rule 2 – Source of personal information	14
Principle / Rule 3 – Collection of information from subject	14
Principle / Rule 4 – Manner of collection of personal information / biometric information	15
Principle / Rule 5 – Storage and security of personal information.....	16
Principle / Rule 6 – Access to personal information	17
Principle / Rule 7 – Correction of personal information	19
Principle / Rule 8 – Accuracy etc. of personal information / biometric information to be checked before use	20
Principle / Rule 9 – Not to keep personal information for longer than necessary.....	21

Principle / Rule 10 – Limits on use of personal information.....	22
Principle / Rule 11 – Limits on disclosure of personal information	23
Principle / Rule 12 – Disclosure of personal information outside New Zealand	24
Principle / Rule 13 – Unique identifiers.....	24
5. Additional Privacy Act Requirements.....	25
Mandatory breach notification requirements.....	25

1. Project Introduction

Foodstuffs South Island Limited (**FSSI**) intends to use facial recognition technology (**FRT**) in its stores for the lawful purpose of protecting the health and safety of staff and customers by reducing serious retail crime by repeat offenders in its supermarkets (**Purpose**). This Privacy Impact Assessment (**PIA**) assesses and addresses the privacy impacts associated with the use of FRT, and outlines safeguards and protocols for the use of FRT in stores.

1.1. Purpose of this PIA

FSSI acknowledges that there are privacy risks associated with FRT. The purpose of this PIA is to:

- (a) identify, evaluate, and manage potential privacy risks arising from the use of FRT in stores; and
- (b) identify strategies and solutions to mitigate and manage those risks to an acceptable level.

This assessment supports FSSI and its supermarkets in complying with their obligations under the Privacy Act 2020 (**Act**), the Biometric Processing Privacy Code (**Code**) and ensures appropriate privacy protections are built into the operation of FRT by FSSI.

1.2. Preparation of the PIA

This PIA was developed to ensure that the use of FRT as a solution to the Purpose - namely, the protection of the health and safety of staff and customers by reducing serious retail crime which includes assaults, the use of weapons, incidents of verbal abuse, threatening behaviour and incidents of disorderly conduct, by repeat offenders (persons of interest, or **POIs**) in FSSI supermarkets (**Retail Crime**) - is aligned with sound privacy practices and controls. The PIA evaluates how personal information (including biometric information) will be managed by FSSI, highlights any associated privacy risks, and recommends privacy safeguards and protections to mitigate or reduce those risks to an acceptable level.

All references to personal information in this PIA will include biometric information as defined in the Code, where applicable.

2. FRT Overview

2.1. Background and reasons for using FRT

Between 2020 and the end of 2024, FSSI experienced a significant and escalating pattern of criminal activity across its supermarket network, with nearly 25,000 criminal offences reported during this period. Notably, the volume of incidents more than doubled—from 3,279 in 2020 to 6,634 in 2024. A substantial proportion of these offences from 2020 to 2024 (77%) have been committed by repeat offenders, highlighting a persistent security challenge.

Retail Crime within FSSI stores also surged during this time, with over 3,300 incidents reported between 2020 and 2024. This included a 70% increase in physical assaults and a 363% increase in the presence or use of weapons from 2020 to 2024. Repeat offenders accounted for 73% of these incidents from 2020 to 2024, underscoring the difficulty in deterring individuals who pose ongoing safety risks to customers and staff.

Additionally, over 2,900 breaches of trespass notices were recorded between 2020 and 2024, further emphasising the limitations of current security measures in effectively enforcing exclusions of known offenders.

FSSI identified 206 individuals who repeatedly engaged in Retail Crime across multiple sites, contributing to over 1,000 recorded events. Of these, 268 incidents involved one or more Retail Crimes. These events were not isolated to a single area but occurred across 38 different stores in 32 suburbs in communities across the South Island, indicating a widespread and mobile pattern of offending.

The geographic spread and recurrence of these incidents underscore the elevated risk posed by these individuals. Their mobility and repeated engagement in serious Retail Crime make it impractical and ineffective to manage risk on a store-by-store basis.

This escalating level of Retail Crime by repeat offenders in FSSI supermarkets poses a significant risk to the health and safety of staff and customers in-store. The multi-regional harm caused by repeat offenders further highlights the need for a coordinated response, at least within the regions or across the network where the harm caused is extreme.

2.2. Methods attempted to address the problem

Currently, FSSI stores try to prevent the recurrence of Retail Crime by repeat offenders by identifying prior offenders based on the memory of its security personnel, which is then verified by authorised personnel using an internal electronic record of CCTV footage. Stores rely on security personnel to remember if an individual on store premises has previously engaged in Retail Crime. This is not an effective or accurate method of identification for several reasons. For example, an individual who has previously engaged in Retail Crime may easily re-enter a store when the relevant security personnel who previously dealt with that individual are not on shift or have otherwise left the store's employment. Individuals may also change their appearance, making it more difficult for security personnel to identify them by mere memory.

To date, FSSI stores have used the following methods, where appropriate, to respond to the increasing prevalence of Retail Crime:

- a. Increased security – increasing the number of security staff both on the floor, and at the entrance during the pandemic and lockdowns, across most stores. Some stores have more security than others depending on their location and at different times, e.g. later hours of Thursday, Friday, and Saturday to deal with Retail Crime caused by alcohol consumption.
- b. In-store training – all customer-facing staff undergo extensive security training with external security consultants that is tailored to the store, including de-escalation, conflict, aggression, and abuse response training.
- c. Body camera technology – this has proven useful in further supporting store staff and security in deescalating situations of Retail Crime and in providing post incident audio and visual recording for review.
- d. Licence Plate Recognition – this has proven useful in identifying vehicles of interest on arrival to a store, enabling store staff to be alerted to the possible presence of a person of interest at the store.
- e. Entry and Exit gates – stores have implemented auto entry and exit gates to and from the supermarket, in order to mitigate the offender's ability to leave the supermarket undetected and often with a trolley or basket of stolen goods, without passing through a checkout.

Despite the use of these methods, the occurrence of Retail Crime (including by repeat offenders) has continued to increase, and as these solutions have not specifically been designed to identify repeat offenders, these methods have failed to effectively identify and reduce the number of repeat offenders. Stores are becoming increasingly concerned, and need solutions to proactively

assist them to identify, record, and manage repeat offenders for the protection of their staff and customers.

In response to this increased risk, FSSI conducted a limited trial of FRT in selected stores during 2025. The aim of the trial was to assess the effectiveness of FRT in assisting with the early identification of repeat offenders and in mitigating the risk of further serious Retail Crime by those individuals.

The trial concluded in January 2026. The key outcomes of the trial included a reduction in known POIs from visiting trial stores, total reportable incidents and Retail Crime decreasing in trial stores, and an increase in reportable incidents in other FSSI stores close to trial stores (showing some displacement of this activity). Additionally, there were zero false positives during the trial, with a 99.6% uptime of the FRT system. The results and performance of the FRT trial were positive, and proved FRT to be an effective solution for the Purpose.

2.3. Proportionality Assessment

FSSI has considered the proportionality of operating FRT in its stores. Based on

- a. the measurable increase in Retail Crime in FSSI stores by repeat offenders;
- b. the material impact that Retail Crime caused by repeat offenders has on FSSI team members and customers;
- c. FRT being used solely for the Purpose;
- d. the effectiveness of FRT in reducing Retail Crime of repeat offenders as demonstrated in the 2025 trial;
- e. FSSI's ability to centrally operate FRT and to put in place technological controls on the sharing of information from the FRT system between FSSI stores and third parties; and
- f. the significant public benefit to FSSI team members in creating a safer retail workplace, and to FSSI customers who come into FSSI stores.

FSSI considers the use of FRT in stores to be a necessary and proportionate solution for the Purpose. FRT has demonstrated benefits that outweigh residual privacy risks from its operation, provided that the privacy risks identified in this PIA are managed to an acceptable level using the privacy safeguards and mitigations set out in this PIA.

2.4. Review and Consultation Process

As part of the PIA, FSSI has reviewed various information sources and carried out a stakeholder consultation process with several internal and external stakeholders. These stakeholders have contributed valuable insights into operational, legal, technical, and risk considerations. Stakeholder consultation included FSSI technology, loss prevention, and legal teams as well as consultation with store owners.

External stakeholders have included the Office of the Privacy Commissioner and Cyber Solutions Limited.

FSSI has taken into consideration the feedback to date to inform its drafting of this PIA and the resulting compliance measures and privacy safeguards in Sections 4 and 5.

FSSI is working closely with Māori stakeholders to continue to develop understanding and be informed of the cultural dimensions of FRT. This includes understanding how the key principles from Te Ao Māori - Rangatiratanga, Whakapapa, Whanaungatanga, Kotahitanga, Manaakitanga, and Kaitiakitanga - and upholding Te Tiriti o Waitangi can be built into FSSI's use of FRT.

FSSI also continues to seek ongoing guidance to ensure Māori data sovereignty and culturally appropriate privacy safeguards are embedded throughout system design and implementation. FSSI has engaged with Te Kāhui Raraunga to learn and understand their Māori Data Governance Model that outlines 8 Pou, and to incorporate the use of each Pou in FSSI's use of FRT and to inform appropriate safeguards for its use of FRT.

FSSI will continue its review and consultation with stakeholders from time to time, and will evolve and update its approach where appropriate in its use of FRT.

3. Use of the FRT System

3.1. The FRT System

The FRT System is made up of the Imagus FRT software from Vix Vizion Pty Limited (**FRT Software**), which will be hosted and managed by FSSI as a centralised system in its own secure instance of AWS cloud, and the Auror platform made available by Auror Limited (**Auror Platform**), which will be hosted by Auror Limited in Microsoft Azure and which integrates and interoperates with the FRT Software via an application programming interface (**API**) made available by Vix Vizion as part of the FRT Software (together the **FRT System**).

Accuracy

FSSI is aware that an FRT system needs to be appropriate for a New Zealand context and population mix. FSSI has chosen a system that is trained on images of people that are similar to the New Zealand population and has a high degree of accuracy.

FSSI will use also other privacy safeguards (e.g. two-person verification) to mitigate the risk of inaccuracy, misidentification and bias.

3.2. How the FRT System Collects and Uses Personal Information

FRT System Personal Information Collection

- (a) Each FSSI store using FRT will have dedicated FRT enabled cameras which will collect facial images of each person who walks into the store. Each facial image will be assigned a biometric template. These templates are matched in real time against a centrally managed watchlist of identified extreme and high-risk offenders (Persons of Interest or POIs) (see below).
- (b) If there is no match, no data is sent by the FRT Software to the Auror Platform and the facial image and biometric template is deleted from the FRT Software within seconds of when the image enters the FRT Software.
- (c) If there is a match, an alert is sent to authorised staff, via the Auror Platform web and/or mobile application, through secure devices for verification. Only qualified matches identified by the FRT Software will trigger alerts to be sent from the FRT Software to the Auror Platform. FSSI will assess and confirm the optimal confidence level for FSSI stores in an operational environment. The alert will contain the name of the POI, behaviour classification, time, store location, and camera image.

- (d) When a match occurs, the detection will remain on the POI timeline within the Auror Platform for 7 years as per Auror retention policy. However, the image will be deleted from the FRT System at midnight on the same day.

Watchlist

- (e) The FRT solution enables stores to receive alerts in respect of POIs in the following risk categories: (1) 'Extreme Threat' and (2) 'High Risk' (the POI Categories).
- (f) FSSI will be using the Auror Platform to manage its POIs and Watchlist (as defined in (j) below), and alert notifications of FRT System matches. The Watchlist will be set up at two levels: a regional level and a South Island wide level. POIs who come within the 'High Risk' POI alert category will be entered on the applicable region watchlist and will be shared and available to FSSI stores in that region using FRT. POIs who come within the 'Extreme Threat' POI alert category will be entered on the South Island wide watchlist and will be shared and available to all FSSI stores using FRT. While 6 out of the top 10 offenders are minors across the FSSI store network, no minors or vulnerable people will be included in the Watchlist.
- (g) FSSI defines 'system rules' for each POI category based on the behaviours / risks they are seeking to target (Watchlist Rules). The Watchlist Rules are configured based on a combination of the timeframe in which the event occurred, and the risk behaviours displayed.
- (h) A person will be labelled an Extreme Threat POI if they were involved in an event in an FSSI supermarket in the last 24 months that displayed the following behaviours:
- a. Physical abuse, and/or
 - b. There is a weapon involved.
- (i) A person will be labelled a High Risk POI if they were involved in an event in an FSSI supermarket in the last 12 months that displayed aggressive behaviour.
- (j) Once defined, the Watchlist Rules are applied to existing POI profiles stored in the FSSI instance of the Auror Platform to identify the list of POIs whose in-store presence they want to be alerted of. If a POI profile meets the requirements of a Watchlist Rule and is approved for enrolment on the Watchlist by a trained and authorised FSSI loss prevention team member (as discussed in (l) below), the individual POI profile is 'tagged' with the relevant POI category that applies to that POI (as discussed in (h) and (i) above) and thereby enrolled on the Watchlist.
- (k) Watchlist Rules are automatically applied to any new POI Profiles recorded in the Auror Platform. This means new POIs can be added to the Watchlist following a store incident where they display Retail Crime subject to the approval of a trained and authorised FSSI loss prevention team member.
- (l) Prior to being added to the Watchlist, each store incident is reviewed by a trained and authorised FSSI loss prevention team members to ensure the incident has been correctly recorded and the POI meet the Watchlist Rules.
- (m) POIs are automatically removed from the Watchlist once applicable events triggering the Watchlist Rules fall outside the selected timeframe. POIs can also be manually removed from the Watchlist by a trained and authorised FSSI loss prevention team member via a

number of methods, including by changing the “tag” associated with a POI and / or setting the POI Profile as ‘sensitive’ (both of which will automatically remove the POI from the Watchlist).

3.3. The Types of Personal Information Collected

The types of personal information that will be collected are:

Category	Data Subjects / Source	Purpose
Facial images (images / video)	All individuals entering the store (captured via instore cameras).	To generate biometric templates for identity matching. This will be captured from existing CCTV streams.
Biometric templates (facial geometry)	Derived from facial images of individuals entering the store and on the Watchlist.	Used to perform real-time facial recognition against a Watchlist.
Match results / alerts	Persons of Interest (POIs).	To notify authorised staff when a POI on the Watchlist is detected.
Watchlist POI profile data (facial image from CCTV image previously stored in Auror Platform and other personal information e.g. name)	Previously identified POIs (via Retail Crime events).	To enrol, classify, and manage POIs based on threat level and incident history.
Incident history metadata	POIs (linked to past Retail Crime in-store e.g. trespass notice information).	To justify Watchlist inclusion and manage behavioural trends.
Behavioural classification tags	POIs	To categorise risk level (e.g., 'Extreme Threat', 'High Risk').
System access logs (e.g. names of match verifiers)	Internal users (e.g., Admins, Security personnel).	To audit user activity and enforce accountability within the FRT System.
Free-text notes by staff	POIs or incident participants.	To document incident context and follow-up actions.
Event metadata (e.g., time, location, camera ID)	General store infrastructure linked to events.	To track when/where incidents occur and support event management workflows.

3.4. The Process if there is an Alert that there is a Match

If the biometric image collected and reviewed by the FRT Software returns a qualified match with an image in the Watchlist:

- a) authorised and trained personnel will receive an alert from the Auror Platform (**FRT Alert**) via web and/or mobile application, through secure devices;
- b) two authorised and trained personnel must verify the accuracy of the FRT System match;
- c) if the match is confirmed as reasonably identical by two authorised and

- trained personnel, the authorised personnel will respond to the FRT Alert and the FRT Alert is updated to confirm the match;
- d) the response will depend on the level of risk identified and the current behaviour of the POI in-store;
 - e) once the incident is resolved, the outcome of the incident will be manually added to the Auror Platform by one of the authorised personnel. This will not include any biometric information (templates) from the FRT Software. All biometric information held in the FRT Software about the verified match is deleted at midnight on the same day of the alert. Once the FRT Alert has been updated, the detection image and FRT Alert within the Auror Platform will remain for 7 years as per the Auror retention policy;
 - f) if the match is not confirmed as reasonably identical by two authorised FRT store personnel, this will be classified as a false positive alert, the new (collected) non-matched image and related biometric template will be automatically deleted from the FRT System after 72 hours.

Note: All authorised FRT personnel that have access to the FRT System and who may receive FRT Alerts will be trained to take measures to verify the accuracy of the alert, and on the process to be followed if there is a misidentification.

3.5. Storage of Personal Information Collected by the FRT System

All personal information collected and stored within the FRT System, including the Watchlist, is stored in Microsoft Azure Australia (by Auror Limited within the Auror Platform) and Amazon Web Services (AWS) NZ/Australia (by FSSI). Auror Limited will process the personal information in the FRT System (excluding the FRT Software, which is hosted and operated by FSSI) solely on behalf of FSSI and stores using the FRT System in providing services to FSSI and stores under its services agreement with FSSI and will not access or use that data for its own purposes.

3.6. Access to the FRT System

Any personal information held in the FRT System will be subject to strict access controls.

In respect of FSSI stores, only authorised staff and store security guards will have access to the FRT System for the Purpose. Store personnel will have no access to the FRT Software and will only have access to the Auror Platform. Staff and security guards will receive training on security and privacy processes. Where the security guards are employed by a third party, the contracting agreement between the store and the security company will be reviewed to ensure privacy obligations are clear.

At FSSI only authorised staff will have access to the FRT System and training will be provided on the security and privacy processes.

All access to the FRT System will be logged and monitored.

Auror Limited's access will be solely as a processor on behalf of FSSI.

3.7. Retention of Personal Information

- (a) As noted above, the facial image and biometric template of an individual that enters a store is deleted from the FRT Software within seconds of when the image enters the FRT System if there is no match with a POI on the Watchlist.
- (b) POIs on the Watchlist are categorised as either Extreme Threat or High Risk. Where a POI is categorised as an Extreme Threat, the data relating to that POI is deleted automatically

- from the Watchlist after 24 months. Where a POI is categorised as High Risk, the data relating to that POI is deleted automatically from the Watchlist after 12 months.
- (c) An audit trail of deletions is maintained in the FRT System.

3.8. Access to and Correction of Personal Information by an Individual

A person may submit an access and/or correction request to FSSI or any FSSI store using FRT to review and correct any personal information about them held in the FRT System. Subject to the Privacy Act, access will be granted once the identity of the requestor is verified. Information will be provided in a manner that is deemed appropriate considering the circumstances and FSSI or any FSSI store's obligations under the Privacy Act.

In addition, FSSI will implement:

- (a) a process to deal with requests to remove a POI from the Watchlist. Any removal of a POI from the Watchlist will be subject to the approval of two members of the FSSI loss prevention team;
- (b) a process for dealing with any misidentifications that take place.

The above processes will be set out in FSSI's FRT operational documents and all authorised FSSI and store personnel (including FSSI and store Privacy Officers) will be trained on these processes.

3.9. Disclosure of Personal Information

Biometric templates cannot be extracted from or disclosed outside of the FRT System.

Personal information held in the FRT System (excluding biometric templates) will be handled and disclosed only in accordance with FSSI's Privacy Policy. FSSI will not otherwise disclose or share images or other personal information generated held in FRT System.

4. Compliance with the Information Privacy Principles

Privacy Principles under the Privacy Act 2020

The Privacy Act is applicable to the processing of the following information in the Auror Platform:

- (a) the name of the authorised store personnel who verify an FRT System alert;
- (b) the name of authorised FSSI personnel who approve enrolment of a POI onto the Watchlist;
- (c) name of the POI (if known);
- (d) trespass notice (if applicable);
- (e) Auror reference "P" number;
- (f) Auror record, including any written reports, incident notes or similar.

Code Rules under the Biometric Processing Privacy Code 2025

The Privacy Code is applicable to the processing of biometric Information, being the facial image and related biometric template, of individuals that enter stores and POIs on the Watchlist generated by or held within the FRT System.

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
<p>Principle 1 – Purpose of the collection of personal information</p> <p>Only collect personal information if you really need it.</p>	<p>There is a risk that more personal information is collected than is necessary for the Purpose.</p>	<p>The FRT System will only collect the personal information specified above.</p> <p>The purpose for collecting personal information using the FRT System is the lawful purpose set out in this PIA.</p> <p>All authorised personnel will be trained in the information that should be entered into the FRT System.</p>
<p>Rule 1 - Purpose of the collection of biometric information</p> <p>Only collect biometric information for a lawful purpose if it is necessary, effective, proportionate, there are no other reasonable alternatives, and reasonable privacy safeguards have been implemented.</p>	<p>FRT may not be effective in reducing harm caused by the Retail Crime of repeat offenders.</p> <p>There are alternative means that have less of a privacy risk that could achieve the lawful purpose (e.g., each store could employ / contract permanent / more security guards / team members to identify repeat offenders when they enter stores).</p>	<p>Refer to the proportionality assessment in section 2.3.</p> <p>FSSI has assessed available alternatives with less privacy risk to FRT and has discounted these as they do not enable FSSI stores to effectively reduce the harm caused by repeat offenders for the reasons discussed in this PIA. However, FSSI will continue to utilise other methods, strategies, processes and tools, alongside FRT, to address Retail Crime in FSSI supermarkets.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
	<p>FRT will collect the biometric information of all individuals that enter stores – this has an inherent risk for those individuals if that information is misused or is accessed in an unauthorised manner. In addition, there is a risk that the authorised FSSI authorised personnel may accidentally enrol a minor or vulnerable person in the Watchlist because they are not able to identify or ascertain if a POI is a minor or vulnerable person (e.g., when a minor does not volunteer their age and reasonably looks older than a minor).</p>	<p>All facial images and biometric templates will be deleted from the FRT Software where they do not match a POI within seconds of entering the FRT Software. No data is sent from the FRT Software to the Auror Platform where there is no match.</p> <p>Enrolment of a POI on the Watchlist will need to meet the criteria, and be approved by trained and authorised FSSI personnel as detailed in this PIA.</p> <p>Store personnel will follow the FRT Alert verification process as detailed in this PIA.</p> <p>All relevant authorised personnel and FSSI and store Privacy Officers will receive FR training, which will include training on, and practicable steps to avoid, misidentification and mitigate against unconscious bias and discrimination in both match verification and enrolment. FR training will take place regularly and a record will be kept on who has been trained.</p>
	<p>FRT could have a disproportionate effect on Māori and Pasifika (and other people of colour) given that the risks of misidentification are potentially higher for Māori and Pasifika individuals (and other people of colour) due to historical examples of FRT systems having lower accuracy in correctly identifying people of colour. Authorised personnel responsible for enrolling individuals onto the Watchlist and / or</p>	<p>FSSI will implement a misidentification process that will be followed in the event an individual is misidentified. This process will include practices and processes that are aligned with tikanga (in particular, tapu, mana, mauri, hau and utu) and ensure that individuals are treated with dignity and respect at all times. FSSI is also seeking ongoing guidance to ensure Māori data sovereignty and culturally appropriate privacy safeguards are embedded throughout system design and implementation. FSSI have engaged with Te Kāhui Raraunga and are utilising their Māori Data Governance Model that outlines 8 Pou, to consider the use of each Pou in FSSI FRT, as well as highlight any safeguarding measures that are in place.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
	<p>verifying a match in an FRT Alert may be biased (either consciously or unconsciously) leading to adverse impacts on Māori and Pasifika individuals (and other people of colour).</p>	
	<p>The mitigations and privacy safeguards set out in this PIA are not adopted or implemented as outlined in this PIA.</p>	<p>FSSI will develop and document operational protocols setting out how the FRT System should be used (i.e., solely for the lawful purpose as described in this PIA). The FRT operational documents will complement the FR training provided to authorised personnel.</p> <p>FSSI will (and will ensure that stores) adopt and implement the privacy safeguards as detailed in this PIA.</p>
<p>Principle / Rule 2 – Source of personal information</p> <p>Get it directly from the people concerned wherever possible.</p>	<p>Personal information and biometric information are collected indirectly by FSSI (in the case of the collected and Watchlist images and related biometric templates) and the stores (in the case of Watchlist images and related biometric templates).</p>	<p>Stores source biometric information directly from an individual when they enter the store.</p> <p>While FSSI and stores indirectly collect personal information and biometric information about individuals, this indirect collection falls within one of the permitted exceptions under this Principle and Rule - namely that it is not reasonably practicable to collect this information directly from the individual in the circumstances.</p>
<p>Principle / Rule 3 – Collection of information from subject</p> <p>Tell them what information you are collecting, what you’re going to do with it, whether it’s voluntary, and the consequences if they don’t provide it.</p>	<p>There is a risk that individuals entering stores may not be aware that FRT is in operation.</p> <p>There is a risk that FSSI and store personnel are not aware that their personal information and biometric information is captured as part of the FRT System.</p>	<p>FSSI has developed a comprehensive FRT policy setting out key information around the scope of FRT operation and collection of personal information, along with the rights of individuals whose information is collected and FSSI’s obligations in handling such information. A copy of the FRT policy will be available for customers on request.</p> <p>Additionally, prominent and clear signage will be displayed at stores before individuals enter into the range of those cameras, to advise individuals entering the premises that FRT technology is in operation, the purpose of the collection of biometric data and how</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
	<p>There is a risk that individuals who are visually impaired may not be able to read the signage and privacy policy informing them about the use FRT in stores.</p>	<p>individuals can obtain more information about the use of FRT.</p> <p>Prominent and clear signage will also be displayed at FSSI supermarkets where personal information is collected about Extreme and High Risk POIs used to populate the Watchlist and shared with stores.</p> <p>Stores will carry out detailed training with their staff and team members to advise them of the FRT technology, the FRT policy, and the scope of how the FRT System will operate at each store. This will include the interaction with the privacy and personal information of customers.</p> <p>A webpage will be created on the FSSI website with information about FRT and with an email address for enquiries. This will include a Factsheet to highlight possible concerns regarding FRT and the facts that align.</p> <p>To the extent possible, where a store trespasses an individual and that trespass notice is for Extreme or High Risk behaviour, store personnel will, at the time an individual is notified they have been trespassed, take reasonable steps to verbally notify the trespassed individual that they may be enrolled into the Watchlist. Given health and safety protocols and the reality that not all individuals who are trespassed will be told at the time they have been trespassed, informing individuals that they might be enrolled in the FRT System may not always be possible</p>
<p>Principle / Rule 4 – Manner of collection of personal information / biometric information</p> <p>Be fair and not overly intrusive in how you</p>	<p>As the FRT Software integrates with a camera that is continuously recording images, the FRT Software will unavoidably capture and analyse images of minors, vulnerable persons and</p>	<p>Signage will be clearly visible explaining FRT is in operation as set out at IPP 3 / Rule 3 above.</p> <p>A Watchlist of POIs will be created who are people who have engaged in Extreme or High Risk behaviour in FSSI stores. The Watchlist POI information is retained for 24 months and 12 months respectively from the time of the applicable incident and then deleted.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
<p>collect the information. Take particular care if collecting information from children or young people.</p>	<p>individuals that are not POIs.</p> <p>Individuals may not be aware that FRT is operating and that their biometric templates are being collected and processed by the FRT System.</p>	<p>Enrolment of POIs onto the Watchlist will be approved by trained and authorised FSSI loss prevent team personnel. No minors or vulnerable people will be included in the Watchlist.</p> <p>All facial images and biometric templates will be deleted from the FRT Software where they do not match a POI within seconds of entering the FRT Software. No data is sent from the FRT Software to the Auror Platform where there is no match.</p> <p>The FRT enabled camera that generates biometric templates that are used by the FRT System will not be placed in any covert locations and will be clearly visible to individuals.</p>
<p>Principle / Rule 5 – Storage and security of personal information</p> <p>Take care of it once you’ve got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.</p>	<p>There is a risk that unauthorised personnel may access personal information or biometric information held by the FRT System.</p> <p>Similarly, authorised personnel may use the personal information or biometric information in an unauthorised manner (e.g. by taking photos on their personal devices).</p>	<p>The FRT Software is stored within a secure encrypted centrally managed enterprise FSSI cloud environment, and the Auror Platform is held by Auror in a secure cloud environment. Access for store personnel is granted or rescinded centrally by designated job roles. Access is only granted to trained and approved personnel within a store. No other FSSI stores can view the data that sits within the FRT System. End users at each store will only get alerts for POIs entering their store.</p> <p>As a condition of employment, all authorised personnel will sign a contractual commitment that they will not misuse, or access by any unauthorised means, any personal or biometric information in the FRT System. If any authorised personnel leaves their employment, then their access to the FRT System will be removed.</p> <p>Auror holds FSSI’s data separately to the data of any of its other customers.</p> <p>Biometric templates cannot technically be accessed or extracted from the FRT System.</p> <p>In addition to the above access controls, access to the Watchlist will be limited to authorised FSSI Loss and Prevention personnel.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>Any FRT images or footage entered to the Watchlist will only be able to be accessed and searched by authorised persons at FSSI for the purposes set out in the FRT operational documents. It will be prohibited for FRT images to be copied or reproduced (e.g. printed out) without the authorisation of the FSSI Loss Prevention Manager.</p> <p>FSSI will periodically audit each store that uses the FRT System, including to:</p> <ul style="list-style-type: none"> • check what information is being collected to ensure stores are complying with FRT operational documents; and review FRT logs to monitor access to the FRT System and personal and biometric information. <p>FSSI will document its audit procedures (and this will form part of the FRT operational documents).</p> <p>FRT images, biometric templates and other personal information about POIs is stored by FSSI on its AWS cloud instance and by Auror Limited (on behalf of FSSI) on its Azure cloud instance, both with servers in Australia. Auror Limited is a NZ company and solely processes the data on behalf of FSSI (not for its own purposes).</p>
<p>Principle / Rule 6 – Access to personal information</p> <p>People can see their personal information if they want to.</p>	<p>There is a risk that individuals are unaware of their right to request and get access to their personal information or biometric information.</p> <p>There is a risk that an individual’s access request is not dealt with in accordance with the requirements of the Privacy Act or FSSI’s FRT operational documents.</p>	<p>The FRT Policy will provide for an individual to request access to their personal information, being any images, video footage and other personal information relating to that individual.</p> <p>Where secondary material is created from the FRT images, for example any written reports, incident notes or similar, this material will also be subject to the Privacy Act where it contains identifiable information about an individual. An individual will be able to request access to such secondary material (subject to any exclusions under the Act).</p> <p>Staff will be trained to respond to these requests.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>FSSI has developed a comprehensive FRT privacy policy setting out key information around the scope of FRT operation and collection of personal information, along with the rights of individuals whose information is collected and FSSI's obligations in handling such information. A copy of the FSSI policy will be available for customers on request.</p> <p>Additionally, prominent and clear signage will be displayed at stores before individuals enter into the range of those cameras, to advise individuals entering the premises that FRT technology is in operation, the purpose of the collection of biometric data and how individuals can obtain more information about the use of FRT.</p> <p>Prominent and clear signage will also be displayed at FSSI supermarkets where personal information is collected about Extreme and High Risk POIs used to populate the Watchlist and shared with stores.</p> <p>A webpage will be created on the FSSI website with information about FRT and with an email address for enquiries. Subject to the Privacy Act, access will only be granted once the identity of the requestor is verified. Information will be provided in a manner that is deemed appropriate in light of FSSI's and each store's obligations under the Privacy Act.</p> <p>FSSI will technically have the ability to access/review the Watchlist in the Auror Platform in order to respond to an access request. It is not technically possible for FSSI to access the biometric templates of the Watchlist images held within the FRT Software.</p> <p>FSSI will ensure that its employee and contractor agreements include appropriate privacy disclosures / consents (which detail that FSSI and stores collect and use personal information of personnel and how authorised</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>personnel can request access to and correction of that personal information).</p>
<p>Principle / Rule 7 – Correction of personal information</p> <p>They can correct it if it's wrong or have a statement of correction attached.</p>	<p>There is a risk that individuals are not aware of their right to request correction of their personal information or biometric information.</p> <p>There is a risk that an individual's correction request is not dealt with in accordance with the requirements of the Privacy Act or FSSI's FRT operational documents.</p>	<p>The FRT Policy will provide for an individual to have the right to correct their personal information where appropriate.</p> <p>Staff will be trained to respond to these requests and will be provided with resources that summarise key privacy related FRT information.</p> <p>FSSI has developed a comprehensive FRT privacy policy setting out key information around the scope of FRT operation and collection of personal information, along with the rights of individuals whose information is collected and FSSI's obligations in handling such information. A copy of the FRT Policy will be available for customers on request.</p> <p>Additionally, prominent and clear signage will be displayed at stores before individuals enter into the range of those cameras, to advise individuals entering the premises that FRT technology is in operation, the purpose of the collection of biometric data and how individuals can obtain more information about the use of FRT.</p> <p>Prominent and clear signage will also be displayed at FSSI supermarkets where personal information is collected about Extreme and High Risk POIs used to populate the Watchlist and shared with stores.</p> <p>A webpage will be created on the FSSI website with information about FRT and with an email address for enquiries. FSSI will technically have the ability to amend the</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>Watchlist in the Auror Platform (including by removing individuals from the Watchlist) in response to a correction request or appeal. Any amendment to the Watchlist on the Auror Platform is replicated in respect of the biometric templates of the Watchlist held in the FRT Software instantly.</p> <p>FSSI will ensure that its employee and contractor agreements include appropriate privacy disclosures / consents (which detail that FSSI and stores collect and use personal information of personnel and how authorised personnel can request access to and correction of that personal information).</p>
<p>Principle / Rule 8 – Accuracy etc. of personal information / biometric information to be checked before use</p> <p>Make sure personal information / biometric information is correct, relevant and up to date before you use it.</p>	<p>The FRT System may incorrectly identify an individual as a match to a POI on the Watchlist.</p> <p>The authorised FSSI personnel may approve enrolment of images of individuals into the Watchlist without context of an incident.</p> <p>Authorised FSSI personnel may upload poor quality images resulting in inaccurate FRT Alerts and/or misidentifications.</p>	<p>There are several steps to ensure the personal information and biometric information is correct before it is used.</p> <p>For the identification of POIs entering an FRT store, the FRT System will be calibrated so a match will only be triggered if it is qualified match with an image of a POI in the Watchlist.</p> <p>Before an alert of a match can be acted on two authorised store personnel must verify and confirm that the image is that of the POI. See Rule 1 above for more information on the verification process that will be followed when the FRT System generates a FRT Alert.</p> <p>Before any personal information or biometric information can be enrolled into the Watchlist, FSSI authorised personnel must: (i) verify and confirm the match and/or that the image is that of the POI; and (ii) take reasonable steps to ensure that the information inputted into the Watchlist is accurate, relevant and not misleading.</p> <p>To mitigate the risk that images enrolled into the Watchlist are not taken out of context, authorised personnel are trained to record a factual description of behaviour at the time</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>of the incident and contextual background into the Watchlist.</p> <p>To ensure that the personal information and biometric information is up-to-date and relevant, where a POI is categorised as an Extreme Threat, the data relating to that POI and incident is deleted automatically from the Watchlist after 24 months. Where a POI is categorised as High Risk, the data relating to that POI is deleted automatically from the Watchlist after 12 months.</p> <p>FR cameras will meet minimum image quality thresholds, and FSSI will regularly review image quality thresholds to ensure the threshold remains appropriate. The Auror Platform is also configured to reject any images that do not meet the predefined quality requirements.</p> <p>The FRT System was tested during the PoC phase and the results showed that it operates as intended.</p> <p>FSSI will regularly review the Watchlist to determine whether a POI should be removed (e.g., for image quality issues, excessive false positives etc.). FSSI will also develop and document in the FRT operational documents:</p> <ul style="list-style-type: none"> (a) a process to deal with requests to remove a POI from the Watchlist. Any removal of a POI from the Watchlist will be actioned by the authorised FSSI loss prevention team; (b) a process for dealing with any misidentifications that take place.
<p>Principle / Rule 9 – Not to keep personal information for longer than necessary</p>	<p>The FRT System may hold personal information and biometric information for longer than necessary if there are not adequate deletion controls put in place.</p>	<p>All facial images and biometric templates will be deleted from the FRT Software where they do not match a POI within seconds of entering the FRT Software. No data is sent from the FRT Software to the Auror Platform where there is no match.</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
<p>Get rid of it once you're done with it.</p>		<p>To ensure that the personal information is up-to-date and relevant, where a POI is categorised as an Extreme Threat, the data relating to that POI is deleted automatically from the Watchlist after 24 months. Where a POI is categorised as High Risk, the data relating to that POI is deleted automatically from the Watchlist after 12 months.</p> <p>When a match occurs, the detection will remain on the POI timeline within the Auror Platform 7 years as per the Auror retention policy. However, the image will be deleted from the FRT System at midnight on same day as the alert.</p> <p>If the match is not confirmed as reasonably identical by two authorised store personnel, the new (collected) non-matched image and related biometric template will be automatically deleted from the FRT System.</p>
<p>Principle / Rule 10 – Limits on use of personal information</p> <p>Use it for the purpose you collected it for, unless one of the exceptions applies.</p>	<p>Principle 10 – personal information may be used by FSSI or store personnel in an unauthorised manner.</p> <p>Rule 10 – CCTV images used in the Watchlist were not originally collected in accordance with Rule 1.</p>	<p>FRT policy sets out the clearly defined lawful purpose for the collection and use of biometric information and personal information via the FRT System (set out above). Biometric information and personal information in the FRT System will not be used for any other purpose.</p> <p>The FRT policy and purposes of use and collection will be reviewed and amended periodically to ensure relevance and compliance.</p> <p>The FRT operational documents will also clearly state the purpose for which the FRT System is to be used.</p> <p>All authorised personnel will undergo privacy and FRT System specific training and refresher courses which make it clear that personal information and biometric information may not be used for any purpose other identifying and responding to POIs. FR training will also detail the privacy</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>safeguards, protocols and processes adopted by FSSI and its stores and set out in the FRT operational documents. The FR training will take place regularly and be documented (with a record kept on who has been trained).</p> <p>System audit logs will be reviewed to validate how Personal Information and biometric information is being used.</p> <p>To mitigate the risk of misuse of personal information and biometric information, the FRT System will be subject to appropriate security and access controls and relevant authorised personnel who have access to the FRT System will provide contractual commitments in relation to the security of the FRT System and use of personal information and biometric information (see Rule 5).</p> <p>In terms of CCTV images originally collected not in compliance with Rule 1, FSSI and its stores have implemented privacy safeguards in respect of that information (as set out in this PIA) and consider that the processing of that information for the Purpose is a proportionate course of action.</p>
<p>Principle / Rule 11 – Limits on disclosure of personal information</p> <p>Only disclose it if you’ve got a good reason, unless one of the exceptions applies.</p>	<p>Personal information or biometric information may be disclosed to unauthorised personnel or disclosed for an unauthorised purpose.</p>	<p>Biometric templates cannot be accessed or extracted from the FRT System.</p> <p>Personal information held in the FRT System will only be disclosed to the individual(s) concerned upon request by them, or where disclosure is required by law (e.g. subject to a Police warrant). FSSI will not otherwise disclose or share images, biometric templates or personal information generated within the FRT System with any third party other than with stores.</p> <p>Auror Limited is a NZ company and solely processes the data on behalf of FSSI (not for its own purposes).</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
		<p>All authorised personnel will undergo privacy and FRT System specific training and refresher courses which make it clear that personal information and biometric information may not be used for any purpose other than identifying and responding to POIs. FR training will also detail the privacy safeguards, protocols and processes adopted by FSSI and its stores and set out in the FRT operational documents. The FR training will take place regularly and be documented (with a record kept on who has been trained).</p> <p>System audit logs will be reviewed to validate how Personal Information and biometric information is being used.</p> <p>To mitigate the risk of misuse of personal information and biometric information, the FRT System will be subject to appropriate security and access controls and relevant authorised personnel who have access to the FRT System will provide contractual commitments in relation to the security of the FRT System and use of personal information and biometric information (see Rule 5).</p>
<p>Principle / Rule 12 – Disclosure of personal information outside New Zealand</p> <p>Only share information with an agency outside New Zealand if the information will be protected.</p>	<p>N/A – there is no ‘disclosure’ of personal information or biometric information to a foreign person or entity.</p>	<p>FRT images, biometric templates and other personal information about POIs is stored by FSSI on its AWS cloud instance and by Auror (on behalf of FSSI) on its Azure cloud instance, both with servers in Australia. Auror is a NZ company and solely processes the data on behalf of FSSI (not for its own purposes).</p>
<p>Principle / Rule 13 – Unique identifiers</p>	<p>FSSI may unintentionally record a unique identifier into the Auror Platform or</p>	<p>The Auror Platform unique identifier (P number) is assigned to an individual to enable FSSI and stores to carry out one or</p>

Privacy Principle / Code Rule	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
Only assign unique identifiers where permitted.	the FRT Software that is assigned by another agency (e.g. driver's license no.).	<p>more of their functions efficiently through use of the Auror Platform. This unique identifier is not used outside of the Auror Platform.</p> <p>The FRT Software assigns unique identifiers (biometric templates) to images. Again, this unique identifier is not used outside of the FRT Software and is created to enable FSSI to deliver a solution to the Purpose and stores to use the FRT System.</p> <p>These unique identifiers will not knowingly be the same as any other unique identifier assigned by another agency.</p> <p>Authorised FSSI and store personnel will be trained not to record any unique identifiers from other agencies within the FRT System.</p>

5. Additional Privacy Act Requirements

Applicable to all personal information and biometric information:

Privacy Act requirement	Summary of privacy risk	Implemented mitigations / privacy safeguards to achieve compliance or reduce risk to an acceptable level
Mandatory breach notification requirements	FSSI or stores may not be aware of unauthorised access or disclosure of biometric information and personal information held in the FRT System such that they will not be able to comply with their mandatory breach notification obligations.	<p>All biometric information and personal information stored within the FRT System will be held by or on behalf of FSSI and stores (and not used for any purpose other than providing services to FSSI and stores). FSSI will (and will ensure that stores) implement strict access controls, including encryption and password protection, and will include appropriate data security and incident notification obligations in its agreements with any third-party contractors (e.g. authorised security personnel) and service providers (e.g. Auror).</p> <p>FSSI's and each store's Privacy Officer and all authorised personnel will be trained on what to do in the event of an accidental or</p>

		unauthorised disclosure of biometric information and / or personal information stored in the FRT System. This process will be set out in the FRT operational documents.
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------