Facial Recognition Technology - Privacy Impact Assessment Report

Updated September 2024

Table of Contents

1. Scope of the Privacy Impact Assessment

1.1 Project Summary

Foodstuffs North Island Limited (**FSNI**) is the franchisor of 328 supermarket stores[1] in the North Island of Aotearoa (**Stores**). Following a significant increase across all Stores in the recorded rates of theft, burglary, robbery, assault (physical and verbal) and other aggressive, violent and threatening behaviour (**Harmful Behaviour**), FSNI and certain Stores (**FRT Stores**) trialled the use of facial recognition technology (**FRT**) for the sole purpose of proactively reducing the incidence of Harmful Behaviour by repeat offenders (**Purpose**).

The preliminary findings from the independently designed and evaluated trial indicate that the use of FRT in the FRT Stores was effective in reducing serious Harmful Behaviour – assaults, incidents of verbal abuse and incidents of disorderly conduct – by repeated offenders.

As such, the FRT Stores intend to continue to use FRT for the Purpose, at least until FSNI receives the final findings from the trial and makes a subsequent decision on any longer term use of FRT.

1.2 Purpose of this PIA

FSNI and FRT Stores understand there are risks associated with FRT from a privacy perspective. The purpose of this PIA is to:

(a) identify any privacy concerns and potential privacy risks arising from the use of the FRT System by FRT Stores; and

(b) identify and provide effective strategies and recommendations to assist FRT Stores in mitigating those risks.

In preparing this PIA, FSNI has taken into account:

(c) the obligations of FRT Stores under the Privacy Act 2020 (**Privacy Act**);

(d) the Office of the Privacy Commissioner's (**OPC**) position paper on the regulation of biometrics released in October 2021 and discussion document entitled *A potential biometrics code of practice* released in July 2023;

(e) the OPC's Privacy Impact Assessment Toolkit;

(f) the OPC's guidance provided on its website in relation to privacy generally; and

(g) the OPC's feedback on FSNI's use of FRT.

1.3 Scope of this PIA

The scope of this PIA is limited to assessing and reviewing the use of the FRT System by FRT Stores for the Purpose, in particular:

(a) how will the FRT System collect and use personal information?

(b) how will the personal information collected by the FRT System be stored?

(c) how will access to the FRT System be managed internally?

(d) how long will the personal information used by the FRT System be retained?

[1] This includes New World, PAK'nSAVE and Four Square.

(e) when and how will the personal information collected, and stored, by the FRT System be disposed of?

(f) how will access requests relating to personal information stored in the FRT System be dealt with by FRT Stores?

1.4 Review and consultation process

As part of the PIA, FSNI has reviewed various information sources and consulted with several internal and external stakeholders, including the OPC and a kaupapa Māori consultancy, in relation to the FRT trial and the use of FRT in FRT Stores more generally.

FSNI has taken into consideration the feedback to date to inform its drafting of this PIA and the resulting compliance measures in Section 4.

The feedback from FSNI's review and consultation process to date has:

(a) confirmed the need to implement an effective tool to proactively address the harm caused to Stores, their staff and customers by the Harmful Behaviour of repeat offenders;

(b) confirmed that FRT has the potential to meet the need identified in (a) above;

(c) allowed FSNI to identify the privacy concerns and risks associated with the use of the FRT System by FRT Stores for the Purpose, including from a Te Ao Māori perspective;

(d) informed the development of business and operational processes and strategies outlined in this PIA to assist FRT Stores in mitigating those privacy concerns and risks.

FSNI will continue its review and consultation process during its use of FRT, and will evolve and update its approach, as appropriate, to the use of the FRT System for the Purpose.

2. Purpose of using FRT

2.1 The problem

Between May 2022 and March 2024, Stores reported that between 31% and 41% of all recorded incidents were committed by repeat offenders.

Internal Store records also show that between January and March 2024, 5,124 separate incidents were recorded, more than double (up 116%) the 2,377 recorded between February and April 2022. During the January-March 2024 period there were 60 separate assaults, up 94% on the previous quarter, mostly on frontline staff and 600 incidents where trespass notices had been breached by offenders, up 17% on the previous quarter.[2]

A list of media reports of crime in supermarkets is set out in **Appendix A**.

Police cannot successfully prosecute repeat offenders unless Stores provide sufficient supporting evidence. To assist Stores to efficiently compile the appropriate evidence from CCTV footage, Stores require a solution that proactively and accurately identifies repeat offenders.

2.2 Methods attempted to address the problem

Stores have tried to prevent the recurrence of Harmful Behaviour by repeat offenders by relying on security personnel to identify repeat offenders, which is ineffective and inaccurate for a number of reasons (including the fallibility of memory and the same security personnel not being on site at all times).

Stores have also tried a number of other methods to respond to the increased prevalence of Harmful Behaviour in Stores generally, such as increasing security and training, improving store layout, electronic tagging and fog canons. Despite the use of these methods, the occurrence of Harmful Behaviour (including by repeat offenders) has continued to increase. As these methods have not specifically been designed to identify repeat offenders, they have also failed to effectively identify and reduce the number of repeat offenders.

Stores are becoming increasingly concerned and need solutions to assist them to proactively identify, record, and manage repeat offenders, allowing them to intervene before any Harmful Behaviour can occur.

2.3 Alternative options for addressing the problem

FSNI has also considered several alternative methods to proactively identify and respond to repeat offenders in an attempt to reduce the recurrence of Harmful Behaviour, such as weapon detection technology and smart CCTV cameras to identify and track suspicious behaviour. Again, these methods do not assist in proactively identifying repeat offenders.

Overall, FSNI and Stores consider that the methods attempted and the alternative options considered are not effective in assisting Stores to proactively identify repeat offenders and reduce the incidence of Harmful Behaviours.

2.4 The solution

FSNI (on behalf of its Stores) identified FRT as an option to assist Stores to reduce the incidence of Harmful Behaviours by proactively monitoring for and identifying

[2] https://www.foodstuffs.co.nz/news-room/2024/Foodstuffs-North-Island-records-doubling

repeat offenders. Until FSNI receives the final findings from the FRT trial from the independent evaluator and makes a subsequent decision on any longer term use of FRT, the use of FRT will be limited to the FRT Stores.

The FRT System (defined below) will assess whether the image of an individual entering a FRT Store matches an image that that FRT Store has identified as a person of interest and, if so, will immediately alert authorised Store personnel. A detailed description of how the FRT System works is provided in Section **Error! Reference source not found.**3.

Imagus by Vix Vizion

FRT Stores will use the Vix Vizion, *Imagus* Facial Recognition Solution (**FRT System**). Founded in January 2011, Vix Vizion is an Australian company that provides facial recognition and video analytics solutions for applications in security, responsible gaming, retail, marketing and transport.

While there is limited public information on the use of the FRT System in New Zealand, in Australia, the Customer Business Services (**CBS**), a division of the South Australian Government's Attorney-General's Department, evaluated and endorsed the FRT System as an approved FRT system to identify previously barred patrons in gaming venues to prevent the recurrence of problem gambling.[3] CBS assessed the FRT System as meeting its minimum technical requirements and Facial Recognition System Provider Requirements.[4]

Accuracy

The National Institute of Standards and Technology (**NIST**),[5] an agency of the US Department of Commerce, has evaluated the accuracy and demographic bias of the FRT System.

NIST tested the FRT System against its global database of facial images and considers that the Imagus FRT System is the second best performing FRT system in the world for processing 'wild' images.[6] 'Wild' images are those where the subject does not pose for the image e.g., images that are taken from CCTV footage.

To mitigate the risk of inaccuracy and bias, FRT Stores will use a number of measures, including the following key measures:

(a) all authorised FRT Store personnel will be trained on the use of the FRT System, including on the concerns relating to privacy, inaccuracy and bias;

(b) the FRT System in each FRT Store will be calibrated to an accuracy level of 90%, meaning only matches with an accuracy rating of at least 90% will trigger an FRT System match; and

(c) two authorised and specially trained FRT Store personnel must verify the FRT System match before any action is taken.

More detail is set out in Section **Error! Reference source not found.**3.

[3] https://www.cbs.sa.gov.au/facial-recognition-technology - search "Imagus".
[4] https://www.cbs.sa.gov.au/sections/LGL/facial-recognition-technology
[5] NIST established a Face Recognition Testing Program in 2000 to provide independent evaluations of both prototype and commercially available facial recognition algorithms. NIST has extensive experience in measuring and reporting on the accuracy and reliability of FRT and has also provided state-of-the-art technology benchmarks and guidance to the FRT industry.
[9] https://www.vixvizion.com/nist-report (June 24, 2022)

3. Use of the FRT System

3.1 How will FRT Stores inform the public about their use of FRT?

To inform customers that a FRT Store is using FRT, each FRT Store will display signage at all entry points (in English and Te Reo Māori) and throughout the store.

All signage will refer to the relevant FRT Store's privacy policy and the FSNI FRT webpage, both of which contain specific information about the use of FRT by FRT Stores, including a list of the FRT Stores. All FRT Store staff will be trained to direct customers, on request, to where they can find more information about the use of FRT and FRT Stores will have an easily accessible physical copy of their FRT Store privacy policy.

3.2 How will FRT Stores collect and use personal information using the FRT System?

FRT System collection

Each FRT Store's FRT System will collect and review footage (facial images) from the FRT System cameras of all individuals that enter that store and will assign a unique, de-identified facial signature to each facial image for matching purposes. This facial signature is referred to as a 'biometric template'.

Where the FRT System does not identify the image as a match with a person of interest (defined below) that is enrolled in the watchlist within the FRT System (**FRT Watchlist**), the image and related biometric templates will be automatically and immediately deleted.

Where a Harmful Behaviour incident occurs in a FRT Store, authorised FRT Store personnel will manually enrol facial images collected by the FRT Store's CCTV system into the FRT Watchlist as set out below.

Matching of facial images

Each biometric template created by the FRT System when an individual enters the FRT Store is matched against biometric templates of POIs in that FRT Store's FRT Watchlist. Each FRT Store's FRT System will be calibrated so a match will only be triggered if it is a 90% accurate match with an image of a POI in the FRT Watchlist. Section 3.4 sets out the measures that stores will take to verify a match. Non match images and related biometric templates will be automatically and immediately deleted.

FRT Watchlist Enrolment

Where a Harmful Behaviour incident occurs in a FRT Store, authorised FRT Store personnel will manually enrol facial images of individuals into the FRT Watchlist from that FRT Store's CCTV footage, if they reasonably believe, based on supporting evidence, that the individual is a Person of Interest (**POI**), being an:

(a) **Offender** – an individual that has:

  (i) engaged in Harmful Behaviour by:

    (A) stealing or attempting to steal from the FRT Store;

    (B) damaging FRT Store product(s) and/or property;

    (C) assaulting (physically or verbally), or behaving in a violent, aggressive, threatening or abusive manner towards, staff and/or other customers; or

(ii) re-entered the FRT Store in breach of their trespass notice; or

(b) **Accomplice** – an individual who has actively assisted an Offender in the commission of Harmful Behaviour, e.g., helps the Offender to flee the FRT Store by driving a get-away car, or hinders FRT Store personnel from responding to the Harmful Behaviour.

Before enrolling a POI in the FRT Watchlist, two authorised FRT Store personnel must take reasonable steps to:

(a) confirm that the individual is a POI; and

(b) ensure that the FRT Watchlist enrolment information is accurate, relevant and not misleading.

Authorised FRT Store personnel are not permitted to enrol any minors or vulnerable persons (i.e., a person with a disability) into the FRT Watchlist.

Any POI who was on a FRT Store's FRT Watchlist during the trial will remain enrolled on that Watchlist until the relevant enrolment period for that POI ends in accordance with this PIA.

3.3 What types of personal information will the FRT System collect?

The FRT System, including the FRT Watchlist, will collect the following types of personal information (together, **Personal Information**):

Functionality	Description
Image	Images of the person captured by the FRT Store's camera system.
Biometric template*	An encrypted digital biometric signature generated from the image. *This is the only additional personal information that FRT Stores will collect that existing systems used by FRT Stores do not.
POI Name	The name of the POI (if volunteered).
Behaviour*	Description of Offender's Harmful Behaviour at the time of incident, e.g., aggressive, abusive, violent, or in the case of an Accomplice, details of how they assisted the Offender. *This information is used so that staff can take appropriate action, should they need to approach or monitor that individual in the future.
Trespass notice reference ID	If applicable, the trespass notice ID. If the FRT Watchlist entry is for an Accomplice, the trespass notice ID of the Offender is also included.
Verifier name	The name of the authorised FRT Store personnel that has verified the enrolment and/or FRT System match.

3.4 What happens if there is a FRT System match?

If the facial image collected and reviewed by the FRT System matches an image in the FRT Watchlist:

(a) authorised FRT Store personnel will receive an alert from the FRT System (**FRT Alert**);

(b) two authorised FRT Store personnel must verify the accuracy of the FRT System match;

(c) if the match is confirmed as reasonably identical by two authorised FRT Store personnel, the authorised personnel will respond to the FRT Alert;

(d) once the FRT Alert is resolved, the FRT Alert is updated to confirm the match and a description of the incident will be manually added to the FRT Watchlist by one of the authorised FRT Store personnel and verified by another authorised staff member in accordance with the process in Section 3.23.2;

(e) if the match is not confirmed as reasonably identical by two authorised FRT Store personnel, the new non-matched image and related biometric template will be automatically deleted from the FRT System within 24 hours..

Note: All authorised FRT Store personnel that have access to the FRT System and FRT Alert will be trained to take measures to verify the accuracy of matches.

3.5 Storage and Retention of Personal Information

All personal information collected and stored within the FRT System, including the FRT Watchlist, is stored in Aotearoa New Zealand.

Where the FRT System does not identify an image as a match with a POI that is enrolled in the FRT Watchlist, the image and related biometric template will be automatically and immediately deleted.

Where a Harmful Behaviour incident occurs in a FRT Store, authorised FRT Store personnel will manually enrol facial images collected by the FRT Store's CCTV system into the FRT Watchlist as set out below.

Personal information stored in the FRT Watchlist is stored for a duration of:

(a) 3 months for an Accomplice; or

(b) up to 2 years for an Offender.

3.6 Security of Personal Information

Any personal information held in the FRT Watchlist will be securely stored in Aotearoa and will be subject to strict access controls.

Only authorised FRT Store personnel will have access to the FRT System for the purposes described in this Section **Error! Reference source not found.**3 and will receive training on security processes. All access to the FRT System will be logged and monitored.

3.7 Disclosure of Personal Information

The FRT Stores will not share any information from their FRT System with any other Stores (including other FRT Stores) or upload any information from the FRT System into any third party programs or applications. In addition, no information stored in the FRT System will be shared with FSNI or other third parties, unless this is required by

law and, in the case of FSNI, to audit FRT Store compliance with the operational protocols set out in this PIA and to assist FRT Stores with responding to privacy access and correction queries. In each case, the information shared will be limited to what is necessary for the purpose of review and will be subject to appropriate confidentiality obligations.

3.8 Access to and correction of Personal Information

A POI may submit an access and/or correction request to the relevant FRT Store to review and correct any personal information about them held in the relevant FRT Store's 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 in light of the circumstances and a FRT Store's obligations under the Privacy Act.

Removal from FRT Watchlist

A person of interest may query their enrolment in the FRT Watchlist by submitting a removal request to privacy@foodstuffs.co.nz.

The email request should set out: (i) the store the incident took place in, (ii) the date and time of the incident, (iii) what happened, and (iv) the reasons why information / image should be removed from the FRT System.

The FRT Store will consider a removal request by reviewing the information provided and assess it against the information it has collected relating to the incident.

4. Compliance with Information Privacy Principles – Privacy Act 2020

Description of Information Privacy Principle (IPP)	Compliance measures
Principle 1 – Purpose of the collection of personal information Only collect personal information if you really need it	The FRT System will automatically delete all images and biometric templates that do not match with a POI (as defined in Section 3.2) immediately following the FRT System making the comparison (which happens almost instantly). FRT Stores will only collect personal information to the extent necessary to identify a match and/or enrol a POI in the FRT Watchlist. Authorised personnel are trained to not enrol any Personal Information of minors, vulnerable persons, and non-POIs in the FRT Watchlist. Authorised personnel will also be trained on how to reasonably ascertain the age of an individual or identify a vulnerable person. Two authorised personnel must verify all enrolments to ensure the personal information recorded in the FRT Watchlist is necessary, accurate and reasonable. Personal Information of POIs within the FRT Watchlist will be automatically deleted in accordance with Principle 9 below.
Principle 2 – Source of personal information Get Personal Information directly from the people concerned wherever possible	FRT Stores will only use the FRT System to collect personal information directly from an individual when they enter a FRT Store. As discussed in Principle 3 below, FRT Stores will take several steps to inform all individuals, where practical, that the FRT System is in operation.
Principle 3 – Collection of information from subject Tell individuals what information you are collecting, what you're going to do with it, whether it is voluntary, and the consequences if they don't provide it.	FSNI has published a FRT webpage which includes information to inform the public about the use of FRT by FRT Stores, including a list of the FRT Stores. FRT Stores will use clear and prominent signage at the entrance of FRT Stores and at appropriate sites throughout the FRT Store to inform all individuals about the operation of FRT and will direct individuals to the online privacy policy and the FRT webpage for further information about what is being collected, who will get the information, and the consequences of not providing the information. All FRT Store staff will be trained to direct customers, on request, to where they can find more information about the use of FRT and FRT

Description of Information Privacy Principle (IPP)	Compliance measures
	Stores will have an easily accessible physical copy of their FRT Store privacy policy.
Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	Two authorised personnel will identify and verify whether an individual's image should be enrolled into the FRT Watchlist. These staff are trained to not enrol any Personal Information of minors or vulnerable persons. The FRT System will automatically delete all images and biometric templates that do not match with a POI immediately following the FRT System making a comparison. The camera that collects images that are used by the FRT System will not be placed in any covert locations and will be clearly visible to individuals.
Principle 5 – Storage and security of personal information Take care of Personal Information once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	Biometric templates cannot be accessed or extracted from the FRT System by FRT Store staff. Access to the FRT System will be subject to strict access controls. As a condition of employment, all authorised FRT Store personnel must sign a contractual commitment that they will not misuse, or access by any unauthorised means, any Personal Information stored in the FRT Store systems. This will include the FRT System. Third party integrators of the FRT System will have no access to the Personal Information held in the FRT System. FSNI will periodically audit each FRT Store's use of the FRT System, including to: • check what information is being collected to ensure FRT Stores are complying with operational guidelines; and • review FRT logs to monitor access to the FRT System and Personal Information.
Principle 6 – Access to personal information Individuals can see their own personal information if they want to	FRT Stores will use clear and prominent signage at the entrance of the FRT Stores and at appropriate sites throughout the FRT Store to inform all individuals about the operation of FRT and to direct individuals to the applicable privacy policy, which outlines an individual's rights to request access to their Personal Information recorded by FRT. All FRT Store personnel will be trained on how to respond to access, correction and removal requests.

Description of Information Privacy Principle (IPP)	Compliance measures
Principle 7 – Correction of personal information Individuals can correct their personal information if it's wrong, or have a statement of correction attached	FRT Stores will use clear and prominent signage at the entrance of the FRT Stores and at appropriate sites throughout the FRT Store to inform all individuals about the operation of FRT and to direct individuals to the applicable privacy policy, which outlines an individual's right to request correction and/or removal of their Personal Information recorded by the FRT System. All FRT Store personnel will be trained on how to respond to access and correction requests.
Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	FRT Stores will take several steps to ensure that the Personal Information enrolled in the FRT Watchlist is accurate before it is used for the Purpose. The FRT System will be calibrated so a match will only be triggered if it is a 90% accurate match with an image of a POI in the FRT Watchlist. Before any Personal Information can be enrolled into the FRT Watchlist, two 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 FRT Watchlist is accurate, relevant and not misleading. To mitigate the risk that images enrolled into the FRT Watchlist are not taken out of context, authorised personnel are trained to record a factual description of behaviour at the time of the incident and contextual background into the FRT Watchlist. To ensure that the Personal Information is up-to-date and relevant, the FRT Watchlist will only hold Personal Information of: (i) Offenders for up to 2 years from the date of enrolment, and (ii) Accomplices for 3 months from the date of enrolment. All other Personal Information is automatically and immediately deleted from the FRT System if the FRT System does not identify a match with a POI. Integrators are hired to install, configure, and implement the FRT System for FRT Stores. The agreements between FRT Stores and integrators will contain contractual commitments from integrators to ensure that the FRT System is correctly implemented and that any issues are promptly remedied.

Description of Information Privacy Principle (IPP)	Compliance measures
Principle 9 – Not to keep personal information for longer than necessary Get rid of personal information once you're done with it	Unless authorised personnel enrol a POI's Personal Information into the FRT Watchlist, the FRT System will automatically and immediately delete all images that the FRT System does not identify as a match with a POI. The FRT Watchlist will only hold Personal Information of: (i) Offenders for up to 2 years from the date of enrolment, and (ii) Accomplices for 3 months from the date of enrolment. After the enrolment period, the information will be automatically deleted.
Principle 10 – Limits on use of personal information Use Personal Information only for the purpose you collected it, unless one of the exceptions apply	FRT Store staff will undergo privacy and FRT System specific training and refresher courses which make it clear that Personal Information may not be used for any purpose other than the Purpose. To mitigate the risk of misuse of Personal Information by authorised personnel, Personal Information is subject to a number of security controls and authorised FRT Store personnel that have access to the FRT System will provide contractual commitments in relation to the security and use of Personal Information. To ensure that Personal Information is only enrolled into the FRT Watchlist for the Purpose for which it was collected, two authorised personnel are required to verify the match and the reason for enrolment before an image is enrolled.
Principle 11 – Limits on disclosure of personal information Only disclose Personal Information if you have a good reason, unless one of the exceptions applies	FRT Stores will only disclose Personal Information held by the FRT System as set out in Section 3.7. FRT Store staff will be provided with privacy training that covers disclosure of Personal Information, and what to do in the event of an accidental or unauthorised disclosure. All authorised FRT Store personnel who will have access to the FRT System will provide contractual commitments that they will not use or disclose Personal Information in an unauthorised manner.
Principle 12 – Disclosure of personal information outside of NZ	Personal Information held by the FRT System is stored only in Aotearoa and is not held or processed by any third-party providers outside of Aotearoa. See more about unauthorised or accidental disclosure under Principle 11. Integrators will have no access to the data held in the FRT System.

Description of Information Privacy Principle (IPP)	Compliance measures
Principle 13 – Unique identifiers Only assign unique identifiers where permitted	The unique identifier assigned by the FRT is not the same as any other unique identifier assigned by another agency. FRT Store staff will be provided with training to ensure that they do not record any other unique identifiers.
Mandatory breach notification requirements	FRT Store staff will be trained on what to do in the event of an accidental or unauthorised disclosure of Personal Information stored in the FRT System.

Appendix A - Media Reports of Store Incidents

Incidents of abuse and assaults on staff and customers across both FSNI and Countdown stores have increased, being reported in both local and global media.

https://www.nzherald.co.nz/nz/supermarket-chain-woolworths-nz-calls-for-new-trespass-laws-as-physical-assaults-on-staff-rise/S4T6P6DYVZGDFEF5KNBP7WLWBM/ (July 2024)

https://www.newshub.co.nz/home/new-zealand/2024/05/foodstuffs-data-reveals-violent-retail-crime-doubled-in-north-island-stores.html (May 2024)

https://www.rnz.co.nz/news/national/514905/woolworths-rolls-out-body-cameras-for-staff-as-assaults-increase (April 2024)

https://times-age.co.nz/business/wta010224supermarketcrime/ (February 2024)

https://www.rnz.co.nz/news/national/507709/new-world-supermarket-security-guard-stabbed-in-auckland (January 2024)

https://www.stuff.co.nz/national/crime/300965536/women-steal-upwards-of-40000-worth-of-groceries-from-auckland-supermarkets (September 2023)

https://www.foodstuffs.co.nz/news-room/2023/GROCERS-REPORT-59-PER-ANNUM-INCREASE-IN-NORTH-ISLAND-RETAIL-CRIME (August 2023)

https://www.stuff.co.nz/national/crime/300959591/supermarket-crime-increases-by-nearly-60-over-past-year-report-shows (August 2023)

https://www.foodstuffs.co.nz/news-room/2023/Grocers-record-almost-40-percent-increase-in-North-Island-Retail-Crime (June 2023)

https://www.nzherald.co.nz/nz/foodstuffs-reports-a-nearly-40-per-cent-increase-in-retail-crime-increase-in-violent-attacks-on-staff-alarming/RXUBEDFOT5GSXMIGHCKLRAHE6E/ (June 2023)

https://www.newshub.co.nz/home/new-zealand/2023/04/smash-and-grab-at-auckland-supermarket-staff-inside.html (April 2023)

https://www.stuff.co.nz/national/126182342/security-guard-allegedly-punched-and-had-trolley-hurled-at-him-during-incident-at-wellington-new-world (August 2021)

https://www.1news.co.nz/2021/09/14/paknsave-security-guard-assaulted-by-woman-who-refused-to-wear-mask/ (September 2021)

https://www.nzherald.co.nz/nz/supermarket-arson-fire-lit-in-trolley-at-west-auckland-paknsave/MEBEMZ64MULPKHEOEZGJ7KQ7AU/ (May 2021)

https://www.newshub.co.nz/home/new-zealand/2021/08/covid-19-north-shore-4-square-workers-praised-for-patiently-dealing-with-inconsiderate-abusive-woman-refusing-to-wear-mask.html (August 2021)

https://www.rnz.co.nz/news/national/450699/man-shot-dead-at-countdown-supermarket-in-auckland (September 2021)

https://www.theguardian.com/world/2021/may/10/dunedin-stabbing-attack-new-zealand-countdown-supermarket (May 2021)

https://www.newshub.co.nz/home/new-zealand/2021/05/reports-of-stabbing-incident-at-supermarket-in-dunedin.html (May 2021)

https://www.nbcnews.com/news/world/new-zealand-police-kill-violent-extremist-after-he-stabs-6-n1278443 (September 2021)