The New Zealand Marketing Association Inc.

Submission to the Justice Select Committee on:

The Privacy Amendment Bill

This submission is made by:

KEITH W. NORRIS

On behalf of John Miles
Chief Executive Officer
New Zealand Marketing Association (Inc)
PO Box 137266 Parnell, Auckland 1151

ABOUT THE MARKETING ASSOCIATION

The Marketing Association (MA) was formed in 1974 and is the industry body dedicated to the marketing profession in New Zealand.

The MA has 8,500 members across brands, marketing service providers, agencies, and suppliers. Each year, we communicate and interact with over 21,000 New Zealand marketing professionals. We have over 30,000 followers across our social media channels, and more than 775,000 annual website visitors.

We are a member organisation of the Advertising Standards Authority (ASA) and our members are required to support strict codes of practice relating to marketing as well as the advertising codes of the ASA.

A major part of our activities involves establishing and promoting codes of practice and best practice guidelines for all forms of marketing communication, including advertising and sponsorship. Many of these codes require an even more stringent observance of fair and responsible data management than the current Privacy Act.

This submission is made on behalf of the members of the Marketing Association.

We wish to reserve the right to make a personal submission to the Select Committee.

WHO ARE OUR MEMBERS?

Our members include major banks, insurance companies, supermarkets, major retailers, telecommunication companies, utilities and Government ministries. A more specific breakdown on member origins from industry sectors is below:

MARKETING ASSOCIATION MEMBERS BY INDUSTRY SEGMENTS

Accounting	Electrical/Electronic Manufacturing	Information Technology and Services	Performing Arts
Airlines/Aviation	Entertainment	Insurance	Photography
Architecture & Planning	Farming	Internet companies	Professional Training & Coaching
Automotive	Financial Services	Investment Management	Political Parties
Banking	Fishery	Legal Services	Public Relations and Communications
Broadcast Media	Food & Beverages	Leisure, Travel & Tourism	Public Safety
Building Materials	Food Production	Logistics and Supply Chain	Real Estate
Business Supplies and Equipment	Fund-Raising	Luxury Goods & Jewelry	Recreational Facilities and Services
Capital Markets	Furniture	Machinery	Research
Chemicals	Gambling & Casinos	Management Consulting	Restaurants
Civil Engineering	Government Administration	Maritime	Retail
Commercial Real Estate	Government Relations	Marketing and Advertising	Sports
Computer Software	Graphic Design	Mechanical or Industrial Engineering	Staffing and Recruiting
Construction companies	Health, Wellness and Fitness	Medical Devices	Supermarkets
Consumer Electronics	Higher Education	Mining & Metals	Telecommunications
Consumer Goods	Hospital & Health Care	Non-Profit Organization Management	Transportation/Trucking/ Railroad
Consumer Services	Hospitality	Oil & Energy	Utilities
Defence & Space	Human Resources	Online Media	Wireless
Education Management	Individual & Family Services	Paper & Forest Products	Writing and Editing

OUR PRIVACY HISTORY

Throughout the last 30 years, the Marketing Association (MA) has been instrumental in driving the adoption of 'best practice' privacy policies for New Zealand marketers.

In the context of this submission, it is important to understand the role the MA has played in the development of the Privacy Act since its introduction in 1993. The association was part of a small group of privacy advocates who assisted the original Privacy Commissioner, Sir Bruce Slane, for 2 years before the Act came into force. The self-regulatory focus for professional marketers has been in place since the early 1990s and following the Code of Practice for direct marketing is a mandatory requirement for all members of the association. Please refer to the code here.

This code contains a requirement to offer consumers the right to opt-out of receiving marketing offers by mail, phone, email:

Here is an extract from the code: 4(b).3 Opting out: In addition to the requirements of the 13 principles of the Privacy Act, consumers must be given the opportunity to 'opt out' of receiving marketing information which they have not requested. Marketers must have a system in place which enables them to honour such requests.

This requirement to offer a voluntary opt-out facility to consumers has been in place for over 20 years and has been the cornerstone of the industry's self-regulation. (NB the Privacy act still has no requirement for opting out of receiving unsolicited communications.) We make this point because we believe that opting out enables consumers to reduce the amount of unwanted or unsolicited communications. Whereas the proposed amendment will increase the number of communications being received.

WHAT IS THE FOCUS OF OUR SUBMISSION?

It is our belief that the Privacy Act 2020 is a well-constructed piece of legislation, which meets the privacy demands of individuals without creating an unnecessarily complex framework for business.

The Marketing Association fully supports the concept of transparency and openness when collecting and using consumer data. However, we have some concerns regarding the proposed amendments to the Privacy Act because of the additional costs and system requirements that would need to be implemented.

We wish to focus on *Part 1* of the Bill which introduces *new information privacy principle 3A* (*new IPP 3A*) relating to the indirect collection of personal information. Under this clause any agency collecting information from a source other than the individual is required to inform that person. Whilst we understand and support the need for openness and transparency in data exchange, we believe this will create expensive and unintended consequences for many small New Zealand organisations including charities, community organisations and small businesses.

WHO IS AFFECTED BY THE PROPOSED CHANGES?

Any organisation which collects personal information about an individual from a source other than from the individual concerned will be affected by the proposed IPP3A. That means anyone collecting, buying, renting or exchanging personal data.

Although we represent a wide range of organisations across the spectrum of New Zealand, we are most concerned with how this amendment will affect the processes and costs of smaller businesses, charities, and community services. Many of these organisations are too small to build their own database of customers and prospective customers. They cannot afford either the systems or the manpower to effectively manage a sophisticated customer relationship management (CRM) system. They therefore rely on acquiring individuals' contact details from data brokers or public sources such as websites. The proposed amendments to IPP3A will create significant cost increases to charities and small businesses in their management of fund raising and customer data management. In most cases they do not have permanent access to third party data, they simply rent it for restricted usage and are contractually prevented from permanently adding contact details to their records. Legislation has an unfortunate habit of financially hitting those that can least afford it.

We therefore recommend that:

1. **Registered charities should be exempt from the requirements of the proposed IPP 3A. and that strong consideration be given to extending the exemption to small business.**

HOW IS PERSONAL DATA ACQUIRED?

Personal contact information is widely available from data brokers who collect information directly from the individual by way of competitions, or business transactions. Many of these brokers are international companies who strictly follow the privacy laws of the countries in which they conduct business. New Zealand organisations, particularly charities, obtain much of their third-party data from brokers based in Australia. These transactions are usually controlled by detailed legal agreements which control how the data may be used. Please refer to example Customer Agreement for List Services included as Appendix 1.

Very little personal data is exchanged commercially on a permanent basis, it is commonly 'rented' for a one only use. So, the data is not permanently collected or held by the recipient, it is simply used to send one direct mail piece or make one phone call. We believe that if personal data is not transferred on a permanent basis, it should not be incumbent on the receiving organisation to go through the processes involved in communicating to the individual concerned.

We therefore recommend that:

2. **Personal contact information obtained from a third party which is the subject of a single use agreement should be exempt from the requirements of the proposed IPP 3A.**

Data brokers may also provide personal contact information for a limited time period. This data may not be kept by the recipient organisation and does not become part of the recipients database unless the individual becomes a customer or donor. In these instances we believe that such transactions should be exempt from the requirements of the proposed IPP 3A.

We therefore recommend that:

3. **Where data is exchanged for a limited time period should be exempt from the requirements of the proposed IPP 3A.**

HOW IS PERSONAL INFORMATION COLLECTED BY DATA BROKERS?

Personal information is often collected by data brokers by way of online competitions. In these cases when the individual enters the competition, they agree to receive future marketing communications. Here is an example of a consent statement from a data supplier based in Hong Kong:

'I consent to the competition's host, its clients and prize sponsors sharing selected information given by me on this site for direct marketing and to contact me by email, phone, text or post with more interesting promotional offers. I can withdraw from this at anytime. For more information please click here.'

In this case the individual has clearly consented to clients and prize sponsors sharing selected personal information. Is it therefore necessary to contact the individual to confirm their personal details have been shared? We think this is an unnecessary duplication and can be annoying to the person concerned.

Similarly, when an individual has been informed at the time of collection that their details will be shared with named organisations, we believe that this meets the requirements of principle 3 of the Act and further notification of collection should not be required.

We therefore recommend that:

4. **When individuals are advised that their information will be shared with multiple named organisations, further notification will not be required under the exemption clause which states 'the individual has previously been made aware of the organisation's collection of the information.'**

SHOULD NAME SUPPRESSION BE MANDATED?

Individual New Zealand consumers will clearly receive more unwanted communications as a result of this amendment bill because organisations will be contacting them to advise that they have received personal data from a third party. This will simply cause annoyance to many thousands of individuals as they will receive continuous notices advising that their data had been exchanged or shared. We do not believe that is the intent of this bill. A far more effective solution would be to allow consumers to reduce the number of unsolicited communications they receive by registering themselves on the MA operated Name Suppression Service (NSS)

For over 20 years the MA has provided consumers the opportunity to opt out of receiving marketing communication through its Name Suppression services. Individuals enter their address and/or 'phone number via the MA website and subscribing organisations use this data to unsubscribe the individuals from marketing communications. Currently over 180,000 consumers are registered on the "Do not Mail' and "Do not Call" database. The NSS also allows subscribing organisations to access the official deaths information through an Authorised Information Sharing Agreement (AISA) between the MA and the Dept of Internal Affairs. This enables those organisations to avoid sending communications to the families of deceased persons.

In its 2011 report on the Privacy Act, the Law Commission supported the use of the MA Name Suppression Service. There is precedent for mandatory use in NZ for the Do Not Call & Do Not Mail registers for Credit Pre-screening of acquisition campaigns under the Credit Reporting Privacy Code – https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/crpc2020/ Schedule 10 – Condition 2(b).

Many European countries have mandatory data suppression services, as does the UK and Australia. In the UK the Mailing Preference service is run by the UK Direct Marketing Association. Organisations subscribe to An MPS licence which gives them access to the Mailing Preference Service (MPS) Register, the official 'do not mail' register in the UK, a service which enables individuals to opt out of unsolicited, personally addressed advertising mail. (Consumers can register with the MPS for free.) The NSS in New Zealand covers addressed mail and also includes telephone numbers.

We therefore recommend that:

5. **The facility to opt-out of receiving unsolicited marketing communications though the MA Name Suppression Service should be ratified in law.**

NAME SUPPRESSION SERVICE DATA TRANSFERS SHOULD BE EXEMPTED

As stated, consumers enter their own personal data onto the Name Suppression Service. This data is then downloaded by organisations who subscribe to the service so that the individuals are excluded from unsolicited marketing communications. It is reasonable to assume therefore that in this case notifying the individual each time their data is downloaded would defeat the purpose of the Name Suppression Service. It would in fact prejudice the purpose of the collection and notification should therefore be exempted by principle 3 (4) (c). However we believe this should be ratified specifically by granting exemption from the requirements of IPP3A.

We therefore recommend that:

6. **Personal details transferred to a third party for the purpose of suppressing those details from unsolicited communications should be exempt from the requirements of the proposed IPP 3A.**

CLARIFICATION REQUIRED

There are some areas of the proposed bill which need clarification. In particular the reasons for exemption:

(A) Non-compliance would not prejudice the interests of the individual concerned:

This provision appears ambiguous. We require further clarification on this issue. While we understand the intent behind this provision is to ensure that individuals are not harmed by non-compliance, however, need guidance to define what constitutes "prejudice" in this context. Specific examples or guidelines to help organisations understand their obligations to ensure protection of individuals' rights are needed.

(B) Compliance would prejudice the purposes of collection:

The provision stating that compliance would prejudice the purposes of collection is difficult to understand. We recommend the notes accompanying the introduction of the bill include examples of where adherence to privacy requirements hinders the achievement of objectives.

(C) Under clause 4 of the proposed amendment organisations are required to advise ‘the name and address of the agency that has collected the information and is holding the information’. Does this require the organisation to advise the details of both the original collector of the information and the current holder of the information?

Thank you for the opportunity to make this submission.

APPENDIX

APPENDIX 1 - EXAMPLE CUSTOMER DATA USE & SERVICES AGREEMENT

CUSTOMER AGREEMENT/DATA USE & SERVICES AGREEMENT
Purchase Order –Licensed Data & Services

Purchase Order ("PO") to the Customer Agreement/ Data Use & Services Agreement with an Effective Date of 10 June 2024("Agreement") between Project Dynamics Limited and XXX Ltd (the "Customer"). This PO forms part of the Agreement between the parties and will be effective as of 10/06/2024 ("PO Effective Date"). Capitalised terms not defined in this PO have the same meaning as they have in the Agreement.

Customer Contact Name: John Doe	
Address: XXXXXXXZ	
Mobile Phone No: XXXXXXXX	**Landline No: n/a**
Email Address: XXXXXXXXXXX	
Delivery Address: (if different from Customer address)	
Campaign/Project: South Auckland Prospecting	

---

1. Term

The term of this PO ("**PO Term**") begins on the PO Effective Date and continues for a period of 3 months.

2. Deliverables

(a) **List Data** - The Customer has requested the following List Data

LIST DATA:
Purpose: Telemarketing
Number of uses: SINGLE USE

CONSUMER LISTS:
On line Opt In survey database, self-reported
Name, Address, Residential or Mobile

SELECTION CRITERIA
One per household
Self-reported Home Owner

Areas and Counts as follows

Town	Suburb		Landline Only	Mobile Only	Landline & Mobile
Takanini			**421**	**42**	**20**
Papakura	**Karaka**		**220**	**16**	**4**
Papakura	**All other suburbs**		**1308**	**121**	**59**
ESTIMATED TOTAL		**1949**	**179**	**83**	**2211**

Data Privacy and Consumer Rights

The supplied data has been washed against the latest versions of the New Zealand Marketing Association Do Not Call, Do Not Mail and Deceased Indexes

Please refer any "Where did you get my name from" questions back to Project Dynamics Ltd. We will contact the consumer and confirm how we have their details and offer them Opt Out options and advise the same to the On Line Survey supplier.

The supplied data must be deleted within 30 days of supply as new entries into the New Zealand Marketing Association Do Not Call, Do Not Mail and Deceased Indexes could have occurred within that time frame

The supplied data may contain seed names which will notify us if this data file is used more than once

Format: Project Dynamics is to supply the Data in: Pipe/Excel format. **Encryption:** Data will be delivered, compressed and password protected using WinZip. For Winzip encrypted files the Customer will require version 9 or above to open the data file.

Password Protection: all files supplied by Project Dynamics will be password protected and password will be supplied verbally where required to Customer Contact/nominated party.

Delivery Method: Licensed Data will be delivered via email

For the purposes of this clause, "Data" means Licensed Data, Third Party Data or Customer Data that is enhanced by Project Dynamics.

Code of Practice for Direct Marketing in New Zealand

This Code was reviewed in February 2014.

This Code has been developed by the Marketing Association (MA). The Advertising Standards Authority (ASA); Consumer Affairs, Ministry of Business, Innovation & Employment; Commerce Commission, the Privacy Commission and Consumer NZ were consulted in the review of this Code of Practice.

All marketers are expected to comply with the principles set out in the Code. The compliance guide sets out actions which can help achieve compliance with the principles. Where the compliance guide is silent on a particular issue, marketers are expected to act in accordance with the spirit and intention of the Code, which is to ensure that consumers' interests are properly protected. Although this code is written for marketers, by reading it, consumers can gain an understanding of the standards expected to be met by marketers.

Definitions

a. Consumers are customers or potential customers, whether they are members of the public, organisations or businesses.
b. Direct Marketing is the process by which consumers are individually offered the opportunity to obtain or purchase goods or services or make charitable donations by email, website, text, mail, newspaper, magazine, radio, television, telephone, or any similar means of communication.
c. Appropriate industry Codes of Practice include the Advertising Codes of Practice of the Advertising Standards Authority (ASA) and all other industry codes endorsed by the Marketing Association.
d. Where the word advertisement is used in the Code, it covers any and all forms of advertising.

This code is based on five basic principles:

Principle 1:
Marketers will comply with the laws and bylaws of New Zealand and all appropriate industry Codes of Practice

Principle 2:
Offers will be clear and truthful and not present a product, service, or offer in a way that could mislead the consumer.

Principle 3:
Orders for products or services will be handled in a prompt and responsible manner.

Principle 4:
Marketers will carry out their business in a socially-responsible manner.

Principle 5:
Marketers will uphold high standards of business practice to generate consumer trust.

Principle 1

Marketers will comply with the laws of New Zealand and all appropriate industry Codes of Practice.[1]

This Code assumes that organisations already comply with all New Zealand Law, including relevant bylaws, and is to establish standards of customer service at or above the minimum legal requirements.

Compliance Guide

Particular attention should be paid to:

1(a) **Consumer Laws**: Organisations involved in direct marketing must pay particular attention to the Credit Contracts and Consumer Finance Act 2003, Unsolicited Electronic Messages Act 2007, Fair Trading Amendment Act 2013, the Consumer Guarantees Amendment Act 2013 and any amendments to these Acts, which all include consumer rights provisions.

NB: From 17 June 2014 the Fair Trading Act will include extended powers covering online and door-to-door sales, unsolicited goods, etc.

1(b) **Individual Privacy**: It is important that direct marketers are familiar with The Privacy Act 1993 and the 12 Privacy Principles included in it. Marketing activities must comply with these principles. See http://www.marketing.org.nz/Category?Action=View&Category_id=1464 for an easy reference guide to implementing the 12 Privacy Principles.

Unless it is obvious from the circumstances, marketers must tell consumers in clear, simple language what information about them is being collected, what it will be used for, who it will be disclosed to (if anyone) and that the customer has the right to access their own information.

1(c) **Advertising to Children**: Marketers must also be aware of and abide by the ASA's Code of Practice for Advertising to Children and the Children's Code for Advertising Food. http://www.asa.co.nz/code_children.php). The term "children" for marketing purposes means all those under the age of 14 years.

1(d) **Liquor and Pharmaceuticals**: Attention is also drawn to the Advertising Codes of Practice for Advertising and Promotion of Alcohol and for Therapeutic Products & Services. Liquor advertisements require a LAPS (Liquor Advertising Pre-Vetting Service) code number, and any product making a therapeutic claim requires a TAPS (Therapeutic Advertising Pre-Vetting Service) code number. The requirements of the Sale and Supply of Alcohol Act 2012 must also be observed.

[1] Industry Codes of Practice and Best Practice Guidelines:

Data Transfer	Direct Marketing Data
Direct Marketing Co-operatives	Email Marketing
Fax Marketing	Mobile Marketing
Search Engine Marketing	Social Media Marketing
Telemarketing	Unaddressed Mail
Role of a Privacy Officer	

Principle 2

Offers will be clear and truthful and not present a product, service, or offer in a way that could mislead the consumer.

Compliance Guide

2(a) **Testimonials**: Testimonials used in any form of advertising must be current, typical and genuine and any claims made must be able to be verified.

2(b) **Disguise**: Marketers must not claim to be carrying out a survey or research when their real purpose is to sell a product or service, or to raise funds.

2(c) **Misrepresentation**: Consumers must not be misled into believing that a marketing communication is news, information, research, public service or entertainment programming when its purpose is to sell goods or services or to seek donations to causes or charities.

2d) **Timeliness**: Descriptions and promises must reflect actual conditions, situations and circumstances existing, to the best of the seller's knowledge, at the time of the promotion.

2(e) **Evidence**: Test or survey data used in any communication must be reliable, accurate and current and must support the specific claim being made. Marketers must be able to substantiate the basis for any claim or comparison and must not imply a scientific, factual or statistical basis where none exists.

2(f) **Identity**: Every offer, communication and shipment of goods must identify the marketer and provide the consumer with sufficient information to be able to contact the supplier or retailer.

2(g) **Disparagement**: Inaccurate information must not be used to harm the reputation of competitors' products, services, brands, advertisements or companies.

2(h**) Representation**: Products or services offered must be accurately and fairly represented.

2(i) **Currency**: Prices quoted in advertisements in New Zealand must be in New Zealand dollars and include GST, unless otherwise clearly stated.

2(j) **Competitions**: When contests or prizes are used to promote the sale of goods, the rules of the contest must be clearly stated, and must comply with The Gambling Act 2003, especially the provisions related to “Sales Promotion Schemes”. Particular attention must also be paid to Principle 3 of The Privacy Act 1993 with regard to the collection and storage of personal data. http://www.marketing.org.nz/Category?Action=View&Category_id=1464

2(k) **Refusal of Offer**: A telephone marketer must provide the consumer with a clear opportunity to refuse any appointment or offer. A definite refusal must be accepted right away, and the call ended. People must not be harassed.

2(l) **Cost and Charges**: The marketer must clearly state the total cost, all relevant terms, conditions and payment plans, plus any extra charges such as delivery or handling costs, including any costs incurred in returning goods. The date on which any contract becomes binding must be specified and the terms must be confirmed in writing within five (5) working days of this date.

2(m**) Description**: Products or services offered in all media must be accurately and fairly described. The terms and conditions of the offer must not be made less clear or unreadable by the use of type size, colour, contrast, style, placement or any other treatment.

2(n) **Advertorial/Infomercial**: Advertorials/Infomercials must be clearly identified as such.

2(o) **Comparative Advertising**: Comparative advertising must not mislead or deceive. The comparisons made must be accurate and must be of 'like' products or services available in the same market.

2(p) **Comparative Pricing**: When comparing prices to those offered by other organisations, the comparison must be based on a price at which the item is offered for sale in the local area or available on the Internet and the basis for comparison must be clear.

Principle 3

Orders for products or services will be handled in a prompt and responsible manner.

Compliance Guide

3(a) **Identity**: Advertisements which invite a reply to a Post Office box, email, website, or telephone number must clearly identify the organisation and should also provide a physical address. In the case of an Internet advertisement, this same information must be easily found on the website page linked to that advertisement.

3(b) **Appointments**: In the case of an appointment for a face-to-face meeting, the marketer must give their name and contact details to enable the customer to change or cancel the appointment.

3(c) **Inertia selling/negative option**: Consumers are not responsible to pay for unordered goods or services, or for their return to the marketer. Goods or services must not be sent or charged for unless a confirmed order has been received from the consumer. If a consumer is required to advise that he or she does not wish to receive any further goods or services, that fact must be made clear in the first offer. Options available for the consumer to do this, e.g. mail, email, via the seller's website, should also be made clear. The silence of a consumer is not enough to indicate they have accepted the goods or services. Buyers must actually state they want to buy.

3(d) **Payment options**: Consumers must be advised in clear and simple language of the available methods of making payments, the security of those payment methods, how to use those methods and any additional costs associated with different payment mechanisms.

3(e**) Processing of payments**: Marketers must maintain efficient and complete records of orders and money received so that they can quickly and accurately answer customers' questions about their orders.

3(f) **Payment security**: Organisations must set up systems to ensure any payment information (e.g. credit card details) is collected and stored securely. The information collected must be accurate, up-to-date and kept only as long as needed for the purposes for which it was collected.

3(g) **Shipment:** All orders must be shipped within the time stated in the advertisement. If no time is stated, they must be shipped within ten (10) working days of the order being received.

3(h) **Shipment delay**: If the order, or any part of it, cannot be supplied within the required time, the customer must be notified promptly and given a reasonable idea of the expected delay. At the same time, they must also be given an opportunity to cancel the order and receive a refund.

3(i) **Returned goods**: Marketers must accept delivery of items returned in good condition within the time specified in their Terms and Conditions.

3(j) **Refunds**: Marketers must maintain efficient and complete records of goods returned by customers. Refunds and exchanges must be sent within ten (10) working days from the time the returned goods are received by the trader.

3(k) **Substitution**: If it is necessary to substitute one product for another, the customer must be given the opportunity to cancel the transaction, unless it was made clear in the advertisement that the marketer might not be able to guarantee the colour/model etc. and the consumer has given their consent to receiving an alternative colour/model.

3(l) **Terms and conditions**: The consumer must be informed of all the terms and conditions before a contract is confirmed.

3(m) **Agreements and contracts**: Copies of all relevant documents, agreements, contracts and/or advice of legal rights must be sent to customers within five (5) working days, commencing from the date of the transaction. Documents confirming an order must provide full contact details of the organisation, including a physical address.

Principle 4

Marketers will carry out their business in a socially-responsible manner.

Compliance Guide

4(a) **Children**: A marketer must not knowingly take orders from children under the age of 14 without adult approval. Note : The Minor Contracts Act 1969 states that “minor means a person who has not attained the age of 18 years. A contract entered into with a minor is unenforceable.”

4(b).1 **Do Not Mail & Do Not Call Lists:** The Marketing Association will maintain Do Not Mail (DNM) and Do Not Call (DNC) Lists containing details of consumers who have requested no unsolicited mail and/or telephone calls.

Marketers must check the Marketing Association’s DNM and/or DNC Lists against any prospecting list they plan to use and suppress from that list any names that appear on the DNM and/or DNC Lists. This does not apply when an organisation communicates with existing members or customers or individuals who have opted in to receiving marketing communications. The DNM or DNC should be matched against prospecting lists each time marketing activities are carried out.

4(b).2 **Deaths Information:** Marketers must also access the Deaths Information through the Marketing Association in order to suppress the names of deceased persons in their customer database(s) and/or any list to be used in a prospecting campaign. In accordance with the agreement between the Marketing Association and the Department of Internal Affairs, subscribers to the Deaths Information must comply with the rules governing its use. They must also adopt audit procedures approved by the Marketing Association to demonstrate that obligations under these terms and conditions are being met.

4(b).3 **Opting out**: In addition to the requirements of the 12 principles of the Privacy Act, consumers must be given the opportunity to 'opt out' of receiving marketing information which

they have not requested. Marketers must have a system in place which enables them to honour such requests.

4(b).4 **Marketing list referrals**: Marketers must not allow individuals to provide details of others (e.g. friends, colleagues, family members) to receive marketing offers without their permission.

4(b).5 **Third party lists**: Marketers using third party lists must ensure the list complies with the requirements of The Privacy Act 1993 http://www.marketing.org.nz/Category?Action=View&Category_id=1464 and the Unsolicited Electronic Messages Act 2007. http://www.antispam.govt.nz/

4(c).1 **Calling hours**: Telephone calls to private homes should only be made between 8.00 am and 9.00 pm, unless the caller is advised that another time would be more convenient and acceptable.

4(c).2 **Calling days**: Telephone marketing calls should be avoided on Sundays and public holidays, unless the caller has a reason to believe that the calls will be readily acceptable.

4(d) **Confirmation of credit card details**: If, while placing an order via telephone, a consumer authorises the charge for goods or services to be made on a credit card, the telemarketer must read back all relevant details of the credit card. They must also be sure that the customer understands that the cost of the goods or services will be charged to the credit card.

4(e**) Verification of Internet orders**: When purchasing over the Internet, consumers must be given an opportunity to check that the details of their orders are correct and be given the right to accept or reject the terms and conditions of the contract.

4(f) **Confirmation of contract/offer**: The receipt of confirmed contracts/offers placed via the Internet or in response to an emailed offer must be acknowledged within 2 working days in order to reassure the consumer that their order has reached its destination.

4(g) **Safety and health warnings**: Where applicable and appropriate, consumers must be given any mandatory safety and health care warnings when purchasing over the Internet or in response to an emailed offer which they would be given at any other point of sale.

Principle 5

Marketers will uphold high standards of business practice to generate consumer trust.

Compliance Guide

5(a) Internal Complaint Handling

5(a).1 **Procedures**: Organisations must have fair and effective procedures in place to handle consumer complaints and queries within a reasonable time and in a way that results in both the consumer and the organisation being satisfied. These procedures will be free of charge to the consumer and will not affect his or her right to seek legal redress.

5(a) 2. **Consumer information**: If asked to do so, organisations must give consumers clear and easy-to-obtain information about complaints handling procedures.

5(a).3 **Dispute resolution**: If a consumer is not satisfied with the way an organisation has handled their complaint and requires independent assistance, they must be provided with the Marketing Association's contact details

5(b) Data Standards

5(b).1 **Collection, management and maintenance of data**: Organisations collecting and storing consumer/personal data should comply with the Best Practice Guidelines for Direct Marketing Data http://www.marketing.org.nz/Category?Action=View&Category_id=1460.
These require that personal information used for marketing purposes is collected, managed and maintained in accordance with best practice standards.

5(b).2 **Data Warranty:** Marketers collecting, storing or using personal data are required to become 'Data Warranted' and thereby entitled to use the 'Data Warranted' trustmark. The Data Warranty Register (DWR) is maintained by the MA and contains the details of all organisations who follow industry best practice in management of personal data. A list of these organisations is published on the MA website.

5(b).3 **Opting out of the Data Warranty**: Notwithstanding the requirements of 5(b).2 above, marketers may elect to opt out of the DWR. For the sake of transparency, a list of organisations who opt out of the DWR will be published on the MA website.

5(c) Marketing By Telephone

5(c).1 **Identity and purpose**: At the beginning of a call, telemarketers must clearly state their name, the organisation they represent and the general reason for their call. If the consumer expresses a wish to end the conversation, then the caller must end the call as soon as possible.

5(c).2 **Identification**: The name and address of the organisation on whose behalf calls are made must be readily able to be verified via the Internet and/or public directories

5(c).3 **Calling line identity:** When making an outbound telemarketing call, organisations must not block the transmission of the calling line identity to any calling number display or any calling name display of a customer who receives the telephone call. Where technically feasible, organisations should ensure that when outbound calls are made from within the organisation, the number which is transmitted or displayed on the receiver's telephone is one which is suitable for return telephone contact by an individual.

5(c).4 **Ex-directory numbers**: Calls must not be made to unlisted or unpublished numbers, unless the consumer has given the calling organisation permission to call them.

5(c).5 **Workplace Permission**: A consumer must not be contacted by telephone on private business at their place of work without permission.

5(c).6 **Source of Personal Information**: When making unsolicited telemarketing calls, organisations must provide, on request, accurate details of the source from which it obtained the customer's personal information.

5(c).7 **Duration**: If a call is expected to take more than three (3) minutes, telemarketers must state honestly how long the call is likely to take. The consumer must be given the opportunity at this time to end the call.

5(c).8 **Cooling-off period**: After a consumer has received any new contract, they must be given a five (5) day "cooling off" period. During this time the consumer may cancel the agreement without being penalised, and any payment or deposit they have made must be promptly and fully

refunded. The consumer is to be told of this "cooling off" period, both at the time the offer is made and in the written contract.

5(c).9 **Recording calls**: Calls may be recorded and the consumer must be advised that this is being done.

5(d) Internet and Other Electronic Media

5(d).1 **Application**: All forms of electronic media, including (but not limited to) the Internet, electronic mail, TXT, mobile phone applications, interactive kiosks, databases and computer-based information services, are covered by these guidelines.

5(d).2 **Spamming**: Unsolicited commercial electronic messages must not be sent by email or TXT or fax unless the recipient has consented to receiving such messages and they are relevant to the existing relationship between an organisation and its customer.

5(d).3 **Internet, email, and TXT message opt-out**: All unsolicited commercial electronic messages must carry a functional 'unsubscribe' mechanism via the same channel and at no cost to the consumer to enable them to opt out of receiving such messages.
Whenever consumers are required to provide personal information on a website, they must be given the opportunity to opt out of having that data made available to others for marketing purposes.

5(d).4 **Reply**: Every electronic commercial communication must clearly identify the marketer and provide the person receiving it with a simple and easy-to-use method of replying.

5(d).5 **Disclosure**: When information is being gathered from individual consumers that could identify them, and which will be linked with clickstream data (such as that obtained from their behaviour, pathway, or choices expressed when visiting a website), they must be advised what information is being collected and how it will be used. This advice must be given before the consumer sends data that could identify them.

5(d).6 Website security

5(d).6.1 Consumers' personal and payment information must be protected by effective security systems.

5(d).6.2 Consumers must be able to access information in clear, simple language about an organisation's security systems.

5(d).6.3 Consumers need to have confidence that they are dealing with a bona fide person or business and that the transaction is also bona fide. Authentication systems, such as digital certificates, should be used to verify the contents of transactions and the identity of the parties where that is necessary and appropriate.

5(d).6.4 Consumers must not be encouraged to provide confidential information in a manner that is considered insecure.

5(d).6.5 All security and authentication processes linked to personal data must be reviewed and updated regularly to ensure appropriate security levels are consistently maintained.

5(e) Protecting the Environment

Whenever practicable, marketers should use renewable or recyclable materials.

Review

This Code was formally reviewed in 2001, 2006, 2008, 2009, 2012 and in February 2014. It will be reviewed at least every three years.

In addition, the Code may be amended between reviews if necessary. Reviews will be carried out by the Marketing Association, in consultation with the Commerce Commission, Advertising Standards Authority, Consumer Affairs, Ministry of Business, Innovation and Employment, the Privacy Commission and consumer organisations.

For Further Information Contact:

NZ Marketing Association
P O Box 47681, Ponsonby, Auckland, New Zealand
Tel: 09 361 7760 Email: contactus@marketing.org.nz

Index to the Code (will be updated once Code signed-off)

APPENDIX 3 – SAMPLE NAME SUPPRESSION SERVICES AGREEMENT

AGREEMENT FOR THE USE OF THE MARKETING ASSOCIATION'S NAME SUPPRESSION SERVICE

Between the **Marketing Association ("MA")** and _____ (the Subscriber) covering the use of the Marketing Association's Name Suppression Service ("NSS") Lists.

GENERAL:

1. The New Zealand Marketing Association maintains separate lists, hereinafter known as the Name Suppression Service ("NSS") to ensure that Marketing Association Members and non-members do not make inappropriate direct marketing approaches. Currently, the lists are:

    i. The DO NOT MAIL List ("DNM") which contains the names and home addresses of persons who have requested no unsolicited marketing communications by mail.

    ii. The DO NOT CALL List ("DNC") which contains the names, home addresses and phone numbers of persons who have requested no unsolicited marketing communications by phone.

    iii. The New Zealand Deaths Information File ("DIF") which contains details of deceased individuals, as provided by the Registrar-General.

    Despite anything else in this Agreement Subscribers may only access and use the DIF as set out in clauses 19 to 22.

2. These lists are made available to Subscribers in accordance with the terms and conditions detailed in this agreement following payment to the MA of the subscription listed in Appendix A.

3. The object of this Agreement is to record the terms and conditions of use, and the parties' agreement that the lists are provided, by subscription, for the sole purpose of suppressing names from outbound marketing communications, and are not to be used for any other purpose; and to provide for audit mechanisms to ensure that no DNM or DNC or Death Information data is ever included in final mail/phone/output files.

TERMS AND CONDITIONS: ALL SUBSCRIBERS

4. The MA is the proprietor of and beneficially owns all the copyright and all other intellectual property rights in the DNM and DNC lists in New Zealand, Australia and worldwide. The MA is also authorised to allow subscribers to access the DIF.

5. The Subscriber will specify which of the lists they require and, upon signing this Agreement, pay to the MA the appropriate annual subscription. The Subscriber is then entitled to receive regular NSS updates from the MA for the purpose of comparing them with any existing and/or future consumer mail or call list maintained/managed by them.

6. The Subscriber agrees to adopt audit procedures approved by the MA to provide assurance that it is meeting its obligations under these terms and conditions.

7. The data or information furnished under this Agreement is for the use by:

    i. Data Service Providers ("DSPs", e.g. a List broker, mail house or bureau managing lists), acting as an agent on behalf of their client/s, who will obtain written agreement from their clients that Name Suppression data will not be duplicated or made available to any other person, in whole or in part in any form or manner whatsoever. Deaths Information may also be supplied to clients on the strict understanding that it is to be used for Name Suppression purposes only.

    ii. Customer List Owners ("CLOs") who will use the information for the purpose of removing or suppressing details of listed persons from their marketing communications.

8. The lists are supplied for suppression purposes only. Subscribers shall

    iii. Flag records as "DNM – Do Not Send" or "DNC – Do Not Call" or similar on their internal database and exclude such flagged records from all outbound communication selections.

    iv. Programmatically exclude all matching records from any outbound communication files prior to output. **At no time shall any data provided as part of the lists be specifically included in whole or part in any database selections.**

9. The lists may not be used for vetting/validating any inbound communication, i.e. specifically filtering or checking an incoming name against the database.

10. DSP Subscribers who use the DNM/DNC/DIF to provide a data cleansing service shall provide to the MA a quarterly report detailing the client organisations for whom they have provided the service.

11. The data is 'seeded' (dummy names included on the lists) to enable the MA to monitor both the mail delivery service and list usage. If the MA receives any communication to a seeded dummy name indicating a breach of these terms and conditions, the MA will be entitled to cease providing updates immediately, and require the immediate return by the Subscriber of any data already provided under this Agreement. These rights are in addition to any other rights the MA has in respect of the data and the Subscriber.

12. While every care is taken to ensure the accuracy of the information supplied, the MA accepts no liability for inaccuracy of information.

13. The Subscriber shall obtain the approval of the MA prior to any wording relating to the use of the NSS lists appearing in print or on the Subscriber's website.

14. Any breach of the above Terms and Conditions may be referred to the Office of the Privacy Commissioner. Pending investigation of any alleged breach, the MA also reserves the right to suspend access to the NSS information.

15. The Subscriber will hold the MA harmless from any liability, loss or cost (including legal fees) arising from any third party claim (including but not limited to a claim from the Registrar-General

of Births, Deaths and Marriages and/or the Crown) that results from any act or omission of the Subscriber in breach of this Agreement.

16. The MA reserves the right to vary these terms and conditions on reasonable notice to the Subscriber.

17. This agreement remains in place until either party receive notice of cancellation. Annual renewal invoice will be issued in the month preceding the month of the subscription start date unless notice of cancellation has been received by either party.

18. This agreement replaces any prior agreements and commences the date the second party signs this document.

TERMS AND CONDITIONS: DIF SUBSCRIBERS

19. The MA authorises its Subscribers to access and use Deaths Information only through the access and use of the DIF via a unique login and password that identifies (at a minimum) the Subscriber.

20. The MA requires its Subscribers to agree to the following minimum terms in relation to the DIF, including in relation to the use or modification of, access to and security of information therein:

    i. Subscribers will nominate to the MA their staff who require access to the DIF. The MA will authorise those staff members only to have login and password rights to download the DIF.

    ii. Those authorised staff members referred to in clause 10i. agree to keep confidential their login and passwords for access to the internet site to download the DIF, so that only authorised staff of Subscribers and the MA requiring access to the DIF may access that information.

    iii. Subscribers agree to use or access information in the DIF for the sole purpose of removing deceased persons' names from Subscribers' phone and mail lists used for unsolicited marketing campaigns.

    iv. Subscribers may use information from the DIF for the purpose of removing or suppressing the names of deceased persons from a database held by the Subscriber. However, Subscribers must not create a permanent record of 'deceased' based on the DIF in their records. For example, records must not be flagged with 'deceased' (or similar); instead they should be flagged as 'do not contact' (or similar).

    v. Subscribers may make minor formatting corrections to their own database to ensure the person whose name is suppressed is accurately identified, provided the purpose of the formatting correction solely advances the purpose for which the information has been provided to the Subscriber (see clause 20.iii)

    vi. Subscribers must not otherwise access, or manipulate or modify information received in the DIF, or compare or match that information with other information.

    vii. Subscribers must not otherwise create a new databank or change or manipulate the information from the DIF into a form different from the form in which it was provided.

    viii. Under no circumstances may a Subscriber disclose the DIF or information from the DIF to anyone else, including another person, body or organisation, or authorise any other party to access, collect, hold, use, modify, collate, disclose, compare, harvest or match or otherwise misuse the information in the DIF except for the sole purpose of removing dead persons' details as outlined in clause 20iii.

ix. Subscribers must ensure information in the DIF is safely stored and held securely. Subscribers must take all reasonable steps to ensure the information they access is protected from any attempts to intentionally or inadvertently access, collect, hold, use, modify, collate, disclose, compare, harvest or match or otherwise misuse the DIF information.

x. Subscribers must securely destroy information provided in the DIF once names have been suppressed or removed from relevant databases, and in no case shall retain any information from the DIF longer than three (3) months after having accessed the DIF.

xi. Subscribers will advise the MA immediately of any circumstances, incidents or events that have jeopardised or may jeopardise the security of the information in the DIF, or have jeopardised or may jeopardise the security of any computer system in its custody that is used to access that Information.

xii. Subscribers are responsible for compliance with the Privacy Act 1993 and section 78F of the Births, Deaths, Marriages and Relationships Registration Act 1995 in respect to the information supplied in the DIF, including in relation to the storage of information.

xiii. Subscribers agree that the MA or its appointed agent can audit their compliance with the minimum requirements.

21. For the purposes of clause 20.i and 20ii. “Staff” means staff of the Subscriber or agents of the Subscriber. The Subscriber must ensure that any such agents are subject to the same minimum obligations that the Subscriber is subject to in clause 20i to 20xiii.

22. The Subscriber acknowledges that the MA has provided written notification to the Registrar-General as to who its Subscribers are, and information as to which country Subscribers are located and in which they store DIF information. The Subscriber agrees that the MA will advise the Registrar-General in writing of any modifications to that information, including in relation to new Subscribers. The Subscriber also agrees that the information may be shared with the Privacy Commissioner.

CANCELLATION: ALL SUBSCRIBERS

23. In respect of the DNM and/or DNC Lists the MA may cancel this Agreement by giving the Subscriber four (4) weeks’ notice of cancellation and, except where the Agreement is cancelled for breach of any of these terms and conditions, may refund any unused portion of the subscription.

24. In respect of the DIF, without penalty the MA may immediately cancel this Agreement by written notice to the Subscriber if the MA's agreement in relation to the DIF with the Department of Internal Affairs is terminated or expires, or if the Subscriber fails to comply with any of the matters set out in clauses 19-22 of this Agreement. Upon termination the Subscriber must immediately cease any access or use of the DIF and, as soon as practicable thereafter and in any event within six (6) months, securely destroy all information provided to the Subscriber via the DIF.

The Subscriber may cancel this agreement by advising the MA in writing. Subject to clause 25 cancellation by the Subscriber will take effect on the annual renewal date unless a prior date is agreed to in writing. No refund will be given.

SIGNATORIES

I …… Title: ……
(please print)

of ……
(Company name)

hereby accept the terms and conditions of Name Suppression Service Agreement.

Signed: …… Date: ……

Signed on behalf of the Marketing Association:

Name: …… Title: ……

Signed: …… Date: ……..

Marketing Association Name Suppression Services
PO Box 137266
Parnell
AUCKLAND 1151

Email: contactus@marketing.org.nz

Appendix A

Annual Subscription Fees

EXCLUDING GST

	CLO	DSP
Deaths Information	$3,895.00	$5,245.00
Do Not Mail List	$1,595.00	$1,895.00
Do Not Call List	$1,595.00	$1,895.00
All	$7,085.00	$9,035.00
Deaths & DNM	$5,490.00	$7,140.00
Deaths & DNC	$5,490.00	$7,140.00
DNC & DNM	$3,190.00	$3,790.00

Members receive a 25% discount off the fees listed above.