

The Marketer's Guide to Applying FISA:

How to Leverage Canada's Newest Internet Law



Introduction

As a marketer you need to be well informed about anything that can have an impact on the success of your campaigns. That is the reason the authors of this Guide – Thindata 1:1, Return Path, the Law Office of Kris Klein a professional corporation and the Coalition Against Unsolicited Commercial Email (CAUCE) – have come together to develop a powerful tool that will help marketers develop more effective campaigns and therefore improve the experience of consumers of electronic messages.

This Guide concisely summarizes the details relevant for marketers about FISA – The Fighting Internet and Wireless Spam Act. But, this document takes one more critical step in helping marketers succeed: it provides actionable guidelines so that you can comply with the new law and use it to optimize your marketing campaign results.

In this Guide, you will find answers to the following questions:

- » [What is FISA?](#)
- » [Do I need to comply?](#)
- » [What do I need to do to comply with FISA?](#)
- » [What are the penalties of not complying with FISA?](#)
- » [What should I do now?](#)

Finally, this Guide includes The **FISA Action Chart** which outlines the steps you can take to ensure that your marketing campaigns comply and optimize the new law. And, to provide you with a relevant basis of comparison, **The FISA Action Chart** also compares the new obligations to those under the CAN-SPAM Act of 2003 – which marketers worldwide have been applying to their campaigns.

What is FISA (Bill C-28)?

FISA, the Fighting Internet and Wireless Spam Act (Bill C-28) introduced by the Canadian government in May, 2010¹, will establish important new requirements for anyone using electronic messaging for marketing in Canada.

FISA will apply to any form of electronic message sent for marketing purposes (referred to as a "Commercial Electronic Message", or "CEM"), including: email, SMS, instant messaging and social media/networking.

FISA also addresses Internet marketing challenges such as malware, phishing, pharming and other Internet threats².

Do I Need to Comply?

Anyone sending a CEM (Commercial Electronic Message) from Canada or to someone in Canada is subject to FISA. Canadian and international organizations sending to Canadians are required to comply with the bill.

What do I need to do to comply with FISA?

FISA requires opt-in consent before marketers can send a CEM. This is consistent with the long-established requirement for opt-in consent under the Personal Information Protection and Electronic Documents Act (PIPEDA) (http://www.priv.gc.ca/information/guide_e.asp). This means that consent must be obtained before a CEM can be sent. There are also a number of circumstances under which consent may also be implied. These include: (i) where the sender has an existing business or non-business relationship with the recipient; (ii) where the recipient has published their electronic address in a prominent manner; (iii) or where the recipient has provided their email address directly to the sender³.

FISA also requires senders to identify themselves, to indicate on whose behalf the message is sent, to provide up-to-date contact information and to include a functional unsubscribe mechanism.

These rules apply regardless of how many messages are sent (i.e. where a single message is sent).

What are the penalties of not complying with FISA?

FISA establishes a civil regime with significant enforcement powers and penalties⁴. Administrative monetary penalties can be as high as \$1 million per violation for individuals, and \$10 million per violation for organizations. FISA also includes provisions for a private right of action that allows any person to seek damages in court resulting from a violation of the law.

FISA enables the agencies responsible for enforcing the law -- the Canadian Radio-television and Telecommunications Commission, the Competition Bureau and the Office of the Privacy Commissioner of Canada -- to work with foreign counterparts in the enforcement of FISA and similar foreign legislation.

The good news for marketers is that these penalties and powers are specifically aimed at the most egregious offenders (i.e., spammers). Organizations that commit an honest mistake while otherwise making reasonable efforts to comply with the legislation have protections under the legislation. Most importantly, the 'due diligence' defence provides that a person should not be held liable for a violation where they can demonstrate that they have exercised due diligence to prevent the commission of the violation. This is further incentive to ensure that your organization understands and complies with the requirements of FISA.

FISA Action Chart

Follow the guidelines described in the following FISA Action Chart to ensure that your marketing campaigns campaign comply and optimize the new law.

MARKETERS' CORE ISSUE: WHAT MESSAGES ARE COVERED

CAN-SPAM

Only addresses email.

FISA covers

- » Unsolicited Email, SMS, Instant Messaging (IM)
- » Spyware, Malware, Phishing, and Pharming
- » Social Networks

How to optimize your campaigns while leveraging FISA

Establish a baseline policy for interacting with your subscribers across all technologies, something that will meet and/or exceed the requirements regardless of the medium.

MARKETERS' CORE ISSUE: WHO A MARKETER CAN SEND EMAIL TO

To ensure your campaigns are compliant with CAN-SPAM

Marketers can send commercial email to anyone. However, marketers cannot send commercial email to anyone who has "unsubscribed" or "opted-out" from commercial email.

To ensure your campaigns are compliant with FISA

Marketers can send email to anyone who has given explicit consent. Consent may also be implied in one of the following circumstances:

- 1) There is an existing business or non-business relationship between the sender and the recipient of the message*;
- 2) The recipient has published their address in a conspicuous manner, and the message is related to the recipient's professional capacity;
- 3) The recipient has provided their electronic address directly to the sender, and the message is related to the recipient's professional capacity.

Explicit consent exists when the recipient provides the sender permission to send messages.

*Definitions of business relationships and non-business relationships can be found at the end of this document.

How to optimize your campaigns while leveraging FISA

Segment your subscribers (and targets) based on expressed preferences, observed behaviors, demographics and customer lifetime value.

Use opt-in consent methods for capturing contact information.

FISA Action Chart

MARKETERS' CORE ISSUE:

WHEN A MARKETER CAN SEND EMAIL

To ensure your campaigns are compliant with CAN-SPAM

Marketers can send commercial email at anytime. But, if an email recipient has unsubscribed, marketers must cease any commercial email within 10 days, and thereafter must receive an explicit request from an email recipient to re-subscribe before sending any more commercial emails to that recipient.

To ensure your campaigns are compliant with FISA

Marketers can send email only after consent is provided, or can be implied.

In most circumstances implied consent lasts for two years.

How to optimize your campaigns while leveraging FISA

Avoid seeking an "ideal" time & day to send email. Only send emails when you have relevant and timely content.

Use preference centers so that subscribers can choose the timing and frequency with which they receive emails.

If you are relying on implied consent, use this two-year window to gather explicit consent.

MARKETERS' CORE ISSUE:

WHAT NEEDS TO BE IN ALL EMAIL MESSAGES

To ensure your campaigns are compliant with CAN-SPAM

Marketers need to include:

- » Valid information in the Email header
- » Company postal address
- » Subject lines that accurately reflect the purpose of the email
- » A functional unsubscribe mechanism

To ensure your campaigns are compliant with FISA

Marketers need to include:

- » The identity of the person who is sending the email message. If the email is being sent on someone's behalf other than the sender, the name of that person needs to be included.
- » Company name
- » Company contact information
- » Easy method of contacting the sender of the message
- » An unsubscribe mechanism

How to optimize your campaigns while leveraging FISA

To increase the likelihood of email being delivered by the Internet Service Providers (ISP), ensure the Domain Naming System (DNS) and the Internet Protocols match the corporate brand sending the email. Also, review the guidelines set out in Thindata 1:1's *The Marketer's Guide to Successful Email Delivery*.

Run tests (e.g. html coding, spam words, subject lines, spelling mistakes, text on graphics, etc.) on your content prior to deploying.

Include your postal address as one of the forms of contact information.

FISA Action Chart

MARKETERS' CORE ISSUE:

WHAT A MARKETER NEEDS TO DO TO ACQUIRE NEW EMAIL SUBSCRIBERS

To ensure your campaigns are compliant with CAN-SPAM

If consent has not been gathered, marketers need to include a notice stating that the email is an advertisement or commercial message. Marketers cannot use address harvesting or dictionary attacks to generate lists.

To ensure your campaigns are compliant with FISA

While FISA does not outline any specific actions, it demands that marketers have consent (either express or implied) prior to sending an email. Marketers cannot use address harvesting or dictionary attacks to generate lists.

How to optimize your campaigns while leveraging FISA

Follow the guidelines set out in the Personal Information Protection and Electronics Documents Act (PIPEDA) and work with your email service provider to take advantage of online contests and offline marketing campaigns. http://www.priv.gc.ca/information/guide_e.cfm.

MARKETERS' CORE ISSUE:

WHAT A MARKETER NEEDS TO DO TO ACCOMMODATE RECIPIENTS WHO DON'T WANT TO RECEIVE THEIR EMAILS

To ensure your campaigns are compliant with CAN-SPAM

Marketers must maintain clear and conspicuous unsubscribe procedures within the email and honor requests for unsubscribing within 10 business days of the request.

Unsubscribe mechanisms must remain active for 30 days from the day the email was sent.

Unsubscribe mechanism must be simple and not require any additional information other than an email address and a preference to opt-out.

To ensure your campaigns are compliant with FISA

Marketers must maintain clear and conspicuous unsubscribe procedures within the email and honor requests for unsubscribing within 10 business days of the request.

Marketers must also provide a method for email recipients to easily contact the person(s) responsible for sending the message. This method must be active for 60 days from the day the email was sent.

How to optimize your campaigns while leveraging FISA

Include an email address unsubscribe and a web page for unsubscribing.

Use a preference centre to ensure that subscribers can opt-out, or opt-down, from individual publications rather than all of your publications. Include 'unsubscribe from all' as an option.

Ask unsubscribers an optional question, "Why are you unsubscribing?" so that you can learn how to modify your campaigns based on this feedback.

Route unsubscribe reports to a customer service representative so that they can be reviewed rather than to an unattended mailbox.

Authors



THINDATA 1:1 (www.thindata.com) is a North American leader in multi-channel database-driven marketing automation technologies and strategic solutions. We help you to cost-effectively engage your customers by leveraging compelling and effective 1:1 dialogue communications – thereby maximizing your revenue growth and ROI. Analytics, predictive modeling and state-of-the-art technologies form the foundation of our solutions. We leverage these insights and tools to uncover opportunities captured in your databases and then deploy the perfect combination of 1:1 marketing messages across online and offline media. Our principle vehicles are email, social media, web, variable dynamic print and mobile.

To ensure that your marketing campaigns achieve your goals while leveraging FISA, contact Thindata 1:1 (1-866-361-3522 ext. 2) or email inquiries@thindata.com.



RETURN PATH (www.returnpath.net) works to make email work better by scoring and certifying email senders from around the world. We help marketers, publishers and other large-volume email senders increase their response rates by providing the world's leading inbox deliverability solution. We help mailbox providers and email administrators at ISPs and enterprises block unwelcome and malicious email by providing near real-time IP reputation scores and other data-driven tools. Taken as a whole, these tools and services improve the consumer experience of email by protecting them from spam, phishing and other abuse. Return Path offers free access to Sender Score, the email reputation measure compiled through our cooperative data network of ISPs and other email receivers, at our reputation portal: www.senderscore.org.

For email deliverability tools and consulting services contact Return Path: rpinfo@returnpath.net.



THE LAW OFFICE OF KRIS KLEIN (www.krisklein.com), a professional corporation, is an Ottawa-based law firm specializing in electronic commerce, privacy, access to information and other federal regulatory issues. The firm has worked with the Canadian government in the development of FISA and related policies.

For practical and effective legal guidance, contact the Law Office of Kris Klein, a professional corporation. Also look for a comprehensive compliance guide, written by the Law Office of Kris Klein, to be published when FISA comes into force. Contact Shaun Brown sbrown@krisklein.com for more information.



CAUCE NORTH AMERICA INC (www.CAUCE.org) was formed in March 2007 in a merger between CAUCE U.S. and CAUCE Canada. CAUCE has moved beyond its original mission of encouraging the creation and adoption of anti-spam laws to a broader stance of defending the interests of the average Internet user against Spam 2.0: Spam, phishing malware & spyware. CAUCE North America is led by a combined board with a cumulative century of experience in the field of Internet advocacy, and is funded by its individual and corporate members.

Endnotes

This Guide is provided for information purposes only, and is not intended as a substitute for qualified legal advice. The authors make no claims as to the absolute reliability and accuracy of any information presented herein, and accept no liability or responsibility for any errors or omissions.

1. Bill C-28 (http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/h_gv00567.html) was formerly Bill C-27, the Electronic Commerce Protection Act (ECPA).

2. Please review “The Digital Economy in Canada” glossary for more details (<http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00333.html>) or consult the authors of this Guide.

3. Both business and non-business relationship are defined at the end of this document. A message can only be sent under the latter two scenarios where the recipient has not expressly stated that they do not wish to receive unsolicited messages and where the message is related to the recipient's professional capacity.

4. Violations of FISA are not criminal offences. Note: The Competition Act includes the ability to prosecute certain violations involving misleading and deceptive practices as either civil violations or criminal offences.

Key Definitions

» You are considered to have had a business relationship when a customer has purchased/leased a product, good or service, bartered or entered a contract with you.

» You are considered to have had a non-business relationship when a person donates to, volunteers for, or becomes an official member of, your organization.

Copyright 2010

This work is licensed under the Creative Commons Attribution-NoDerivs 2.5 Canada License. As a result you are free to copy, distribute and transmit this document under the following conditions: 1) You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work); and 2) You may not alter, transform, or build upon this work. For more details see <http://creativecommons.org/licenses/by-nd/2.5/ca/>.