Athistha (Nop) Chitranukroh
Of Counsel
athistha.c@tilleke.com

Spam and the Computer Crimes Act 2017: What Do Businesses Need to Know?

As the government seeks to elevate Thailand to the status of a high-income nation, the formation of a digital platform through the "Thailand 4.0" project is seen as an essential element of economic transformation, with the focus now fixed firmly on enhancing research and development, science and technology, and creative thinking and innovation.

To facilitate this economic change, the government and the National Legislative Assembly have made a number of changes to the law, including updates to the Computer Crimes Act (CCA) which were enacted earlier this year. The Ministry of Digital Economy and Society is responsible for issuing subordinate regulations under the CCA.

Spam e-Message Offense

Section 11 of the old CCA previously prohibited sending to another person any email or computer data that concealed or forged its source in a manner that disturbed the normal use of another's computer system. However, it did not apply to disturbing or bothering the recipient themselves. The new version has been amended in direct response to developments in tech-related activities, and now makes it an offense to send an email, or computer data, in a manner that disturbs the recipient and that does not allow the recipient to opt out or unsubscribe.

> "the new version . . . makes it an offense to send an email, or computer data, in a manner that disturbs the recipient and that does not allow the recipient to opt out or unsubscribe"

In addition, the Minister of Digital Economy and Society has issued a notification under the new section 11 that sets out the characteristics and methods of sending emails and data, and characteristics of computer data or e-mails, which are not considered to cause a disturbance to the recipient. This notification acts as a set of "Safe Harbor Rules" for business operators when sending e-messages to their customers, prospective customers, or even to business partners or third parties.

Safe Harbor Rules

The notification defines a "sender" as any person who intends to send company data or emails primarily for commercial purposes, and any website, application, and social media operators that advertise or support the sending of such data or emails. However, it does not include telecommunications business operators that act as intermediaries for transmitting such data or emails.

The following types of e-messages are assumed not to cause a disturbance to the recipient.

1. An e-message sent to another person as evidence of an agreed contractual transaction, or for compliance with law, or for expressing a relationship or a legal relationship between each other.
2. An e-message sent by a government body that enforces the law, for the purpose of providing communications that are not for commercial purposes.
3. An e-message sent by an educational institution, a charitable body, or other organizations, which is not for commercial purposes.
4. An e-message sent in a legal manner which does not violate any individual rights and which is not for commercial purposes.

The notification states that e-messages for commercial purposes (and not within the scope of 1–4 above) are only permissible when consent has been obtained from the recipient, and the following conditions are met:

- E-messages must specify the signs, details, and processes that will enable the recipient to opt out of or unsubscribe from receiving such e-messages, including technical measures allowing the recipient to do so quickly.
- After a request to unsubscribe has been made, the sender must suspend the sending of e-messages to the recipient immediately or, in certain circumstances, within seven days from the receipt of the request.
- It is strictly prohibited for the process or request form for opting out/unsubscribing to be conditional or to divert for any additional commercial purposes (for example, if clicking the opt-out request routes the user to other websites or other sales distribution channels).
- If the sender continues to send e-messages to the recipient after a request has been made, the recipient may send another request, in writing, by way of an email, registered mail with return receipt, or any other way by which they can confirm receipt. If the sender continues to send e-messages after receiving a request of this nature, the sender is deemed to be committing the spam offense under section 11 of the CCA.

Practical Issues

It remains to be seen how the requirements can be complied with in practice. For example, some businesses have asked how they should get consent from the recipient and whether implied consent could be acceptable.

Since this spam e-message offense could attract a maximum fine of THB 200,000 per spam communication, companies that engage in online business activities need to proceed with caution in their electronic marketing and adhere to the safe harbor rules in order to avoid exposure to potential regulatory penalties.

Though the notification provides further guidance and clarification on the spam e-message offense and what business operators should do to avoid committing it, there will still be a number of practical issues on compliance, going forward, that will require further interpretation. The notification grants the Permanent Secretary of the Minister of Digital Economy and Society the power to interpret and consider any issues resulting from any actions that arise from the notification, and companies would be well advised to be alert for any such interpretations in the near future.