From: Jason Slattery [mailto:jasonsl@rogers.com]
Sent: Wednesday, June 29, 2011 3:50 PM
To: George Hungerford
Subject: Comments regarding proposed amendments to National Policy 11-201 Delivery of Documents by Electronic Means

June 29, 2011

Attention: George Hunderford

Regarding: proposed amendments to National Policy 11-201 delivery of electronic documents

Dear George:

To begin with, I want to thank you for the opportunity to comment on this matter. There are three areas on which I am submitting my comments.

In terms of the proposed changes, I would first like to recommend a change in Part 3 - Miscellaneous electronic delivery matters / 3.2 Confidentiality of Documents. That section currently reads as follows:

"Some documents that may be sent by electronic delivery, such as trade confirmations, are confidential to the recipients. Deliverers should take all reasonably necessary steps to ensure that the confidentiality of those documents is preserved in the electronic delivery process."

In my opinion, the second sentence does not go far enough because it is too vague. The phrasing "take all reasonably necessary steps to ensure that the confidentiality of those documents is preserved" appears to be well intentioned... but really has no strict and clear implications. What should we consider "reasonable"? The second sentence is not a very useful guide to help those who are unsure of what is allowed and not allowed. At this point, I would like to refer you to a specific web page of the Office of the Privacy Commissioner of Canada's website: http://www.priv.gc.ca/information/guide/auth_061013_e.cfm .

In particular, I would like to draw your attention to paragraphs five and six under the heading "Risks and Threats". Specifically, the following excerpt:

"If e-mail is used, multiple factor authentication processes, "one-time" passwords or shared secrets and public-key certificates, would manage this threat and greatly reduce the risk to both the individual and the organization."
This more clearly spells out what is needed. The reference to "public-key certificates" is clearly discussing the use of digital ID certificates for secure, authenticated email communication. In other words, we are talking about the need to encrypt and digitally sign email communications and all attachments in order to protect the confidential information and to authenticate the sender and the message itself. In my opinion, the wording of the second sentence should be more like the following: "... Deliverers should take all reasonably necessary steps to ensure that the confidentiality of those documents is preserved in the electronic delivery process by the use of both encryption and authentication measures." This removes the ambiguity while still leaving the option of how to encrypt and authenticate the message at the sender's discretion (i.e. it's not service-provider specific or technology specific.)

I understand that the proposed legislation is attempting to accomodate valid current and future technologies and approaches towards secure communication. As the proposed legislation currently stands, it simply does not go far enough. My opinion is that the wording must be adjusted in some way so that it is clearly understood by all who read it that what we are really talking about is encryption. All electronic communications traveling over the Internet must be encrypted if privacy is to be protected. Unless encryption is clearly stipulated, there will be many

who are confused as to what is "reasonable" and what is "not allowed". Businesses/consumers can then pick a secure encryption service that meets their specific needs while at the same time making it abundantly clear that regular (non-encrypted) email is not an option when sending private and confidential documents back and forth over the Internet.

To conclude on the first matter, I also find it odd that one of the most important sections (i.e. protecting the client's private information) is listed in a "miscellaneous" section of the legislation--when we have a Privacy Law currently in effect.

Secondly, I would like to see some expansion and clarification on one of the agreed upon definitions. In "1.1 Definitions -- In This Policy".... you define "electronic signature" as "electronic information that a person creates or adopts in order to execute or sign a document and that is in, attached to or associated with the document." The reason for my concern is that there is a difference between an electronic signature and a digital signature but sometimes we use such terms interchangeably.

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used where it is important to detect forgery or tampering. An email message or electronic document can be digitally signed by a sender's digital ID certificate to ensure that the recipient can confirm that the message/document was sent from a specific person's computer and that the message/document was not tampered with en route.

Whereas an electronic signature is a broader term that refers to any electronic data that carries the intent of a signature. For example, it could include the process of when a consumer pays for a purchase at the local grocery store using a credit card but then must 'sign' on a digital pad and special pen that records the motion of the hand written signature and then shows the results on a viewing monitor--the results of which are then associated with the customer's credit card details. On the other hand, it could also be when a consumer hand writes their signature on to a piece of paper, scans that onto their computer and then saves it as a picture file--which could then be attached (pasted) to a digital form as a 'signature.' These two examples are vastly different in terms of the level of security involved but both fall under the category of 'electronic' signature.

My point is that, when creating legislation and/or guidelines for the industry, it will likely prove very important to differentiate what you mean by "electronic signature" in terms of what is considered secure and acceptable... and what is not. The definition you provided is accurate... but does it imply that all electronic signatures are valid, secure, trusted and acceptable? If that is not what you are implying, then it should be spelled out as to what would be acceptable. From my position as an investment advisor, I would not be willing to accept a 'copy' and 'paste' approach for a signature on an electronic form from a client... because I cannot be certain of the authenticity and consent (in other words, anyone with a copy of the signature and a computer scanner could end up 'signing' forms.) Whereas a 'digital signature' version of an electronic signature would be more acceptable because of the complex mathematical process involved which (with current technolgy) cannot be falsified. Of course, a person then needs to take care that their digital ID certificate is protected... but I digress.

Thirdly, the stated purpose of this legislation is to "provide guidance to securities industry participants who want to use electronic delivery to fulfill delivery requirements in securities legislation." This includes part (2) that says: "We want provisions of securities legislation that impose delivery requirements to be applied in a manner that accommodates technological developments without undermining investor protection."

The above is certainly in the public's best interest. However, I would like to add that your proposed legislatin should be expanded to include all aspects of electronic communication that takes place behind-the-scenes once the investor has agreed to provide their private information. For example, electronic communications containing the investor's private infomation that are sent

by the investment advisor to their head office; between advisors and compliance departments; between the advisor and authorized third parties that involve the client(s)--like approved investment lenders, for example. All of these electronic communications should be protected through encryption but this is an area that is commonly omitted by vague corporate "privacy policies" that do not necessarily cover email messages.

Some people think that simply obtaining the client's signature on a "disclaimer" providing the sender with permission to email confidential information is sufficient. Unfortunately, in my opinion, I don't think the general public is aware of the high level of risk they are taking on by providing such permission (identity theft, etc.) It also puts the company in the unpleasant position of acting in a hypocritical fashion. On the one hand they proclaim that they protect the public's private information through a privacy code.... only to then ask the public for written permission to put their private information at risk in an un-protected email. Encryption is the only way to address a privacy concern.

Thank you for your time.

Sincerely,

Jason Slattery, BA

Investment Advisor
Equity Associates Inc.

Telephone: 506-460-8316
Fax: 506-206-0710