

Summary of CAFII's Virtual Meeting with BCFSa to Discuss the Extra-Provincial Incident Reporting Guideline

On August 9, 2024, CAFII met with the British Columbia Financial Services Authority to discuss the regulator's Extra-Provincial Incident Reporting Guideline.

In attendance from BCFSa:

- Rob O'Brien, Manager, Financial Institutions Policy
- Steven Wright, Senior Policy Analyst, BCFSa
- Ming Hu, Senior Risk & Financial Analyst, BCFSa

In attendance from CAFII:

- Keith Martin, CAFII – *Executive Director*
- Robyn Jennings, CAFII – *Research Analyst*
- Sara Belanger, Assurant
- Rebecca Saburi, BMO Insurance
- Jason Beauchamp, Canada Life Insurance
- Dallas Ewen, Canada Life Insurance
- David Self, CIBC Insurance
- Karyn Kasperski, RBC Insurance – *CAFII EOC Chair*
- Charles Maclean, RBC Insurance
- Christine Suaza, RBC Insurance
- John Burns, Securion Canada – *EOC Vice-Chair*
- Andrea Stuska, TD Insurance
- Fay Coleman, TD Insurance – *Market Conduct & Licensing Vice Chair*
- Shahnoor Khimjee, TD Insurance

CAFII's Executive Director, Keith Martin, began the meeting by thanking BCFSa and remarking on the regulator's willingness to collaborate and engage in dialogue. BCFSa explained that, initially, it had the intention to require reporting incidents to include filling out a form unique to BC, but after discussion with industry BCFSa concluded that other existing forms like OSFI's that met the data requirements for BC could be used instead.

The BCFSa walked CAFII through the guideline so that the CAFII members in attendance could provide feedback and/or input. Steven Wright (Senior Policy Analyst, BCFSa) began the presentation by explaining how, in 2022, the BCFSa proposed an incident reporting rule requiring extra-provincial insurance and trust companies to report material information security incidents. Industry was concerned with this proposal, stating that they should be allowed to voluntarily comply with reporting expectations rather than through a rule. Industry stressed that due to the requirements to file multiple reports at a time when an incident has occurred, efforts should also be made to harmonize requirements. In response, this requirement now outlines the expectations regarding reporting material information security incidents by extra-provincial insurers and trust companies through a Guideline, not a rule, and the Guideline is focused on harmonizing requirements, to the extent possible, with other federal and provincial regulators. Mr. Wright

informed CAFII that they have also been working with CCIR on a harmonization document that would develop one set of requirements across all provincial and territorial regulators. Finally, he added that the purpose of the consultation is to obtain industry feedback on the new draft Guideline, ensure industry comprehension, and respond to any questions.

Looking closer at the guideline's components, Mr. Wright explained that, for the incident reporting form, the BCFSa has identified the required data points that need to be shared with BCFSa. He is confident this aspect is harmonized with other jurisdictions, except for the additional request to identify the number of BC-resident customers affected by the reporting. They have not specified an exact form to be filled out, rather BCFSa has identified the data points that need to be reported on, which should be allowing regulated entities to fill out an existing form that they already need to submit to a regulator, like the OSFI form.

In terms of timelines for reporting, the BCFSa is asking that extra-provincial companies notify the regulator as soon as possible within reason, but no later than 72 hours after determining that an incident is material. This does *not* mean the full report is sent in 72 hours after an incident, rather it means that BCFSa will be notified within 72 hours that an incident meets the materiality threshold. K. Martin mentioned a recent incident – the crowd strike outage – and asked the regulator if that was an example of a material event that companies would need to report on. Mr. Wright said yes, that is one example, and whether an outage meets the threshold depends on how long a company is offline. Mr. Ming explained that BCFSa was proactive during the crowd strike outage and reached out to companies to determine the magnitude of the impact.

David Self (CIBC) asked if there was any subjectivity around reporting for the 72-hour deadline after determining materiality. Mr. Wright replied that, yes, there would have to be subjectivity, but BCFSa would always fall back on the “reasonable persons test” or the idea that the person reporting the incident had exercised reasonable judgment. BCFSa went to some lengths to emphasize that they intended to be reasonable and they were expecting best efforts from industry if an incident had occurred.

In terms of transmitting these reports, the regulator understands that these reports can include very sensitive information, therefore, it has taken measures to ensure security and confidentiality around filing them. BCFSa has, specifically, established a process in which, in the event of an incident, the company will contact the regulator via email explaining it wants to submit an incident report. The BCFSa will get back to the company with a secure SharePoint link so the report can be uploaded safely. The BCFSa is currently working on creating a mailbox specific to incident reporting. Once the mailbox has been created, the Guideline will be updated to include the new address.

Mr. Wright mentioned that the Guideline discusses materiality and what constitutes a material event. Ultimately, determining meeting the materiality threshold comes down to a company's judgement as informed by the guideline. Again, the regulator assumes companies will exercise reasonable judgment to determine materiality.

K. Martin asked the regulator what it intends to do with the reports it receives and what industry might expect in terms of interactions with the regulator regarding process and expectations. Steven Wright explained that the primary, but not sole, focus will be on the market conduct implications of an incident for BC residents. The BCFSa and its market conduct team acknowledge its limited capacity and will, therefore, need to triage the reports it receives and assess each event's significance to determine the severity of the incident, and the degree of action required by BCFSa in response. Regarding timing, the BCFSa is conscious of burdening companies; it does not believe that communication and/or actions will occur immediately after an incident but rather only after companies have gotten control over the incident.

CAFII EOC Chair, Karyn Kasperski (RBC Insurance), suggested the BCFSa assign one individual during the triage process to handle communication with a company to avoid repetition and confusion. BCFSa responded that this is the goal, however, it is a small regulator and will not always have the resources necessary to do so. BCFSa will try to streamline the process as much as possible.

Charles McLain (RBC Insurance) explained that his company has been in conversation with OSFI around incident reporting, and it has stated that it considers brokers and MGAs to be relevant third parties and thus their breaches need to be reported by the insurers they have contracts with. He then asked if, in BCFSa's eyes, there is an onus on insurers to report when MGAs inform them about an incident, even if the insurer's system is untouched. The BCFSa replied that, according to the Guideline's objectives, if the MGA is providing frontline services to customers (as stipulated in the contract between an insurer and MGA that establishes duty of care to customers), then yes, it needs to be reported. BCFSa will not require the level of detail OSFI requires but will need to receive basic information.

Finally, BCFSa informed CAFII that it has not determined a publication date for the Guideline, however, when it does, it will inform CAFII and its members.

K. Martin thanked BCFSa for its transparent and informative conversation.