Appendix 5 – Text of Amendments to section 3703 of the IIROC Rules (Clean)

Section 3703 of the IIROC Rules is hereby amended as follows:

IIROC Rules
RULE 3700 **REPORTING AND HANDLING OF COMPLAINTS, INTERNAL INVESTIGATIONS AND OTHER REPORTABLE MATTERS** … **Part A - REPORTING REQUIREMENTS** … **3703. Reporting by a Dealer Member to IIROC** (1) For purposes of this section 3703, a "cybersecurity incident" includes any act to gain unauthorized access to, disrupt or misuse a *Dealer Member's* information system, or information stored on such information system, that has resulted in, or has a reasonable likelihood of resulting in: (i) substantial harm to any *person*, (ii) a material impact on any part of the normal operations of the *Dealer Member*, (iii) invoking the *Dealer Member's* business continuity plan or disaster recovery plan, or (iv) the *Dealer Member* being required under any *applicable laws* to provide notice to any government body, *securities regulatory authority* or other self-regulatory organization. (2) A *Dealer Member* must report to *IIROC* any of the following matters, within the time period and using the method prescribed by *IIROC*: (i) all client complaints, against the *Dealer Member* or any current or former *Approved Person*, except service complaints. For the purpose of clause 3703(2)(i), a service complaint by a client is one that is related to service issues and is not the subject of any domestic or foreign *securities laws*, (ii) whenever an internal investigation is commenced by the *Dealer Member* in accordance with section 3706, (iii) the results of the internal investigation under clause 3703(2)(ii),

IIROC Rules

(iv) any time the *Dealer Member*, or a current or former *Approved Person* is subject to one of the following in any jurisdiction inside or outside of Canada, while in the employ of the *Dealer Member* or concerning matters that occurred while in the employ of the *Dealer Member*:

(a) charged with, convicted of, plead guilty or no contest to, any criminal offence,

(b) named as a defendant or respondent in, or is the subject of, any proceeding or disciplinary action alleging contravention of any *securities laws*,

(c) named as a defendant or respondent in, or is the subject of any proceeding or disciplinary action alleging contravention of the requirements or policies of any regulatory or self-regulatory organization, professional licensing or registration body,

(d) denial of registration or license by any regulatory or self-regulatory organization, professional licensing or registration body, or

(e) subject to a civil claim or arbitration notice involving any of the following:

(I) any matters related to securities,

(II) any matter related to handling of client accounts or dealings with clients, or

(III) any matter that is the subject of any legislation, rules, regulations, or policies concerning securities, exchange contracts or financial services of any securities or financial services regulatory or self-regulatory organization in any jurisdiction,

(v) the resolution of any matters set out in clause 3703(2)(iv),

(vi) any internal disciplinary action that is taken by a *Dealer Member* against an *Approved Person* as a result of:

(a) a client complaint within the meaning of clause 3703(2)(i),

(b) a securities related civil claim or arbitration notice,

(c) an internal investigation,

(d) a *Dealer Member* initiated disciplinary action imposing suspension, termination, demotion, or trading restrictions on the *Approved Person*, or

(e) a *Dealer Member* initiated disciplinary action not involving any of the matters listed in sub-clauses 3703(1)(vi)(a) through 3703(1)(vi)(c), which results in a monetary penalty:

(I) over $5,000 for a single occurrence,

(II) over $15,000 in total in a calendar year, or

(III) imposed three times or more in a calendar year,

(vii) any *cybersecurity incident*, in writing,

(a) within three calendar days from discovering a *cybersecurity incident*, and must include the following information:

IIROC Rules
(I) a description of the *cybersecurity incident*, (II) the date on which or time period during which the *cybersecurity incident* occurred and the date it was discovered by the *Dealer Member*, (III) an preliminary assessment of the *cybersecurity incident*, including the risk of harm to any *person* and/or impact on the operations of the *Dealer Member*, (IV) a description of immediate incident response steps the *Dealer Member* has taken to mitigate the risk of harm to *persons* and impact on its operations, and (V) the name of and contact information for an *individual* who can answer, on behalf of the *Dealer Member*, any of *IIROC's* follow-up questions about the *cybersecurity incident*, (b) within 30 calendar days, unless otherwise agreed by *IIROC*, from discovering a *cybersecurity incident*, and must include the following information: (I) a description of the cause of the *cybersecurity incident*, (II) an assessment of the scope of the *cybersecurity incident*, including the number of *persons* harmed and the impact on the operations of the *Dealer Member*, (III) details of the steps the *Dealer Member* took to mitigate the risk of harm to *persons* and impact on its operations, (IV) details of the steps the *Dealer Member* took to remediate any harm to any *persons*, and (V) actions the *Dealer Member* has or will take to improve its *cybersecurity incident* preparedness. **3704. Failure to report** (1) Failure to report, as required by sections 3702 and 3703, may result in *IIROC* imposing an administrative fee, or other penalties that are permitted under *IIROC requirements*, against the *Dealer Member* or *Approved Person*. **3705. Reserved.**