Publisher's Note

An Update has Arrived in Your Library for:

Please circulate this notice to anyone in your office who may be interested in this publication. *Distribution List*
☐
☐
☐
☐

THE LAW OF BANKING AND PAYMENT IN CANADA
Bradley Crawford, Q.C.
Release No. 1, April 2026

What's New in this Update:

This release features a new Chapter 46, "Cyber Risk Management".

Thomson Reuters®

Customer Support
1-416-609-3800 (Toronto & International)
1-800-387-5164 (Toll Free Canada & U.S.)
E-mail CustomerSupport.LegalTaxCanada@TR.com

Highlights:

Cyber Risk Management in Canadian Banking: Regulatory Foundations, Contractual Tools, Emerging Threats, and Global Standards—Introduction—This commentary examines the obligations and best practices for technology and cyber risk management within Canadian banking law. It reviews OSFI Guideline B-13 (July 31, 2022), OSFI's self-assessment framework (November 3, 2025), and the private-law mechanisms through which FRFIs can structure cyber-risk allocation within borrower documentation and third-party arrangements. It also evaluates the risks posed by emerging AI-based adversarial methods and aligns Canadian practice with global frameworks developed by the IMF, BIS, CPMI-IOSCO, and BCBS.

Cyber Risk Management in Canadian Banking: Regulatory Foundations, Contractual Tools, Emerging Threats, and Global Standards—Cyber Insurance as a Risk Transfer Mechanism—Cyber insurance has become an increasingly important residual risk-transfer tool for FRFIs operating in Canada. Although OSFI does not mandate cyber insurance under Guideline B-13, its principles-based emphasis on proportionality, operational resilience, and layered controls permits the strategic use of insurance as part of an institution's broader technology and cyber risk management program.

Cyber Risk Management in Canadian Banking: Regulatory Foundations, Contractual Tools, Emerging Threats, and Global Standards—Canadian FRFIs: Losses, Liability and Supervisory Consequences Arising from Cyber-Related Incidents—Cyber incidents involving Canadian FRFIs have produced tangible financial losses, class-action exposure, and heightened supervisory expectations. While OSFI has not publicized civil monetary penalties in the manner of some foreign regulators, FRFIs have incurred direct remediation costs, settlement payments, and ongoing compliance obligations under OSFI's Technology and Cyber Security Incident Reporting Advisory and Guideline B-13. Public testimony and press reporting confirm a material increase in high-impact incidents, with OSFI noting that reported "priority one" events at banks rose from ~10 (2022) to 28 (2023), underscoring both the prudential and litigation perimeter for cyber events in Canada.