National Banking Law Review

General Editors: Blair Keefe and Eli Monas, Torys LLP

VOLUME 32, NUMBER 4 Cited as 32 Nat. B.L. Rev. AUGUST 2013

• PRIVACY CLASS ACTIONS IN CANADA: ARE PLAINTIFFS BANKING ON FINANCIAL INSTITUTIONS? •

Patrick Flaherty and Molly Reynolds
Torys LLP

For years, North American legal commentators have been warning that privacy class actions would proliferate. As these warnings become reality, what kinds of privacy class actions are being launched and in what circumstances? How far are the claims proceeding? On what basis are they settling? Have class members recovered compensation from courts? Do the "deep pockets" of financial institutions make them targets for these kinds of lawsuits? And although financial institutions are often defendants in privacy actions, will we see more privacy actions with financial institutions as plaintiffs? These questions all merit consideration.

Privacy class actions have long been on the rise in the United States, and they are increasingly common in Canada. Generally, the class action landscape can be divided into two distinct categories of privacy claims: (1) claims arising from mishaps or crime and (2) claims challenging business practices.

Both types of claims engage privacy concerns and present liability risks for businesses, but the legal and strategic issues may be different. The effect of a challenge to a financial institution's business practices could be wide-ranging. The harm caused by accidents and criminal schemes can be difficult to anticipate and costly to an organization's reputation and bottom line, but this harm may not affect the organization's business model. Both scenarios must be taken seriously by financial institutions, which must collect, use, and disclose sensitive customer

• In This Issue •

LexisNexis

information in the ordinary course of their business.

There are also broader issues to consider. Although recent developments demonstrate that litigants and legislatures are increasingly concerned about the security of personal information, the lack of demonstrated harm from most alleged breaches leads some to question whether the legal system should be engaged at all.

Class Actions Arising from Mishaps

Privacy class actions often arise as a result of the inadvertent transmission of customer information.[1] They have also been triggered by the improper disposal of personal information (*Pinero v. Jackson Hewitt Tax Service Inc.*).[2] Recently, a class action was commenced in Ontario, alleging that Ford Motor Company of Canada had uploaded the personal information of approximately 10,000 current and former employees to an unsecured website maintained by an external information technology vendor. The claim seeks $14 million in damages for increased risk of identity theft and costs of preventing theft, damage to credit reputation, mental distress, and time and costs of engaging in precautionary measures to protect class members' credit information.[3]

In the U.S. case *Jackson Hewitt Tax Service Inc.*, the plaintiffs commenced a class action against the second-largest professional tax service firm in the world for allegedly disposing of its customers' tax returns in a public dumpster. Someone fished the returns out of the dumpster and contacted local media and law enforcement. Although Jackson Hewitt alleged that the documents were stolen, it remains unclear how the documents came to be disposed of in such a public location.

In another U.S. example, AOL was sued for alleged breaches of federal electronic privacy law after it temporarily and accidentally posted nearly 20 million keyword searches of approximately 658,000 AOL members on a public website. Certain keywords contained personally identifiable information.[4]

In Canada, cases have also arisen from accidental disclosure of personal information through the simple mistake of leaving a document in the wrong place,[5] even when it could not be determined how many people had seen the information, whether it had been copied, or whether it was used to the plaintiffs' detriment. Misplaced portable electronic storage devices are a frequent cause of alleged privacy breaches. In 2008, a class of plaintiffs commenced a claim after UPS lost a data tape belonging to DaimlerChrysler Financial Services Canada while it was en route to a credit-reporting agency.[6] In 2011, the Ontario Superior Court certified a $40 million class action after a public health nurse lost a USB key containing personal information about people who had been vaccinated against the H1N1 flu virus.[7] In 2012, the court approved a settlement whereby each class member will be compensated for demonstrable economic harm as determined by an adjudicator, and class counsel will be paid $500,000 for costs and disbursements.[8]

Most recently, in December 2012, an employee of Human Resources and Skills Development Canada (HRSDC) misplaced a USB key containing the personal information of over 5,000 people, including each person's social insurance number, medical information, birthplace, level of education, occupation, and local Service Canada processing centre. While carrying out an official probe of the missing USB key, the privacy commissioner's office

discovered that HRSDC had also misplaced an external hard drive containing the personal information of nearly 600,000 student loan borrowers, including each borrower's name, social insurance number, date of birth, address, and student loan balance.[9] Class actions have been filed in Ontario, Newfoundland, and Alberta.[10]

The frequency of similar incidents should serve as a reminder to businesses to have in place policies about transporting customer information on portable electronic storage devices and to implement safeguards such as encryption where appropriate. The federal Privacy Commissioner has issued Guidelines to organizations responding to privacy breaches.[11] HRSDC introduced a new policy banning portable hard drives within the department and prohibiting people from connecting unapproved USB keys to the computer network. HRSDC is also introducing new data-loss-prevention technology and a disciplinary policy for failure to follow privacy and security codes.

Class Actions Arising from Crime

Crime can result in major data breaches. Class actions have arisen from the theft of portable devices with databases containing sensitive personal information,[12] the disclosure of customers' e-mail addresses to third parties who subsequently send spam mail,[13] and the interception of consumer data by hackers.[14]

In *LaRose c. Banque Nationale du Canada*,[15] the Québec Superior Court authorized a class action relating to the theft of three laptops, one of which contained personal information of a group of mortgagors. More recently, customers of Honda Motor Company and Honda Canada launched a class action seeking $200 million in damages for breach of contract, breach of privacy rights, and negligence. The claim alleges that Honda ought to have known that its computer database, which contained personal information of North American and Japanese customers, was vulnerable to hacking by unauthorized third parties and that it failed to take adequate security measures. The lawsuit also alleges that Honda's business model and privacy policies contributed to the damages alleged by the class members.[16] Claims arising from business practices are discussed in more detail below.

In Re Heartland Payment Systems, Inc.[17] arose from one of the largest data breaches ever reported. The U.S. payment processor faced a total of 17 consumer class actions and 10 bank and credit unit class actions arising from a security breach when, in 2007, hackers breached Heartland's computer security, using malware (malicious software). The hackers, who have since been convicted on criminal fraud charges, stole approximately 130 million credit and debit card numbers and corresponding personal information.

Both consumers and financial institutions filed claims against Heartland, which included allegations that Heartland failed to uncover the security breach until notified by third-party credit card companies, delayed notifying customers, and did not offer the affected individuals credit monitoring services or other relief. Heartland settled with the major credit card companies in 2010, paying out approximately US$100 million. The banks' claims were dismissed, and consumers settled for US$4 million. The claims of the banks and credit card companies in *Heartland* highlight a potential developing trend in Canadian class actions: financial institutions as plaintiffs when third parties' loss of personal information may affect the institutions or their customers.

Privacy class actions arising from crime typically allege negligence in developing and maintaining security measures to protect against data breaches. Some actions allege breach of an express or contractual term in the agreement between the business and the customer. In some cases, the focus of the claim is not the mishap itself but the subsequent delay in notifying customers and the appropriate authorities, thus preventing them from taking steps to mitigate harm arising from the breach.

Class Actions Arising from Business Practices

Privacy class actions have also challenged companies' business models and practices relating to handling personal information. Online services that actively encourage users to provide, use, and share personal information are particularly exposed. An increasing number of litigants claim to have a reasonable expectation that businesses will protect their personal information, especially sensitive financial information. They claim that a business's use or disclosure of personal information has exposed them to harms including identity theft, harassment, embarrassment, and mental distress.[18]

These claims typically allege that the company

- acquired, used, or disclosed customers' personal information without prior authorization or consent;
- contravened its own privacy policy; or
- diverted users' private data to third-party providers of targeted advertising for profit.

In Canada, attempts have been made—unsuccessfully to date—to challenge business practices, using privacy class actions. In *Union des Consommateurs c. Bell Canada*,[19] a proposed class action was brought in Quebec against Bell Canada on behalf of Internet subscribers who complained about Bell's alleged "throttling" practices. The claim alleged that Bell violated subscribers' privacy rights by using a technology called "deep packet inspection" to collect the content of all messages sent by subscribers using Bell's Internet service. The Québec Superior Court declined to certify the action after finding that Bell's technology was used merely for traffic management and not to inspect the contents of the data.

More recently, however, the Québec Superior Court certified a class action against Apple Inc. for collecting and sharing Quebec iPhone and iPad users' personal information without their consent. The representative plaintiff alleged that the class members would not have purchased, or paid as high a price for, the Apple devices if they had known that certain free applications offered by the company could be used to collect and share their personal information with third parties and that the Apps drained the devices' resources without the users' knowledge. The representative plaintiff did not seek damages arising from the alleged breach of privacy itself or claim that the personal information collected had been misused by Apple or any third party.[20]

In other jurisdictions, challenges to business models have had a limited amount of success. In response to privacy complaints, in December 2012, German regulators ordered Facebook to allow pseudonyms[21] contrary to Facebook's business decision to spurn Internet anonymity in favour of requiring users to identify themselves. Facebook has declared an intention to "vigorously" appeal the ruling. Facebook has also faced legal challenges to its practices, which relate to privacy in the United States. In April 2011, a plaintiff filed a class action regarding

Facebook's practice of incorporating users' information and photographs into advertisements. The claim alleges that this advertising technique is wrongful and carried out without user consent. In an attempt to settle the class action, Facebook has announced that it is willing to distribute $20 million to not-for-profit Internet privacy advocacy groups.[22]

One U.S. example is a privacy class action against Michaels, an arts and crafts retail chain, regarding its practice of automatically collecting customers' zip codes during credit card transactions. The suit alleges that by recording customers' zip codes, Michaels is infringing consumer rights established under the Massachusetts *Unfair Trade Practices Act*, which restricts the collection of "personal identification information" during credit card transactions. The ultimate outcome of the action is not yet known, but the plaintiffs achieved an early victory on questions of statutory interpretation. Adjudicating a preliminary motion, the Supreme Court of Massachusetts held that zip codes constitute personal identification information within the meaning of the Act. The court also held that the Act addresses privacy rather than identity theft; therefore, for the plaintiffs' claim to succeed, it is not necessary that they demonstrate damages resulting from identity fraud.[23]

The advent of cloud computing presents another area where businesses must adequately address privacy concerns when designing their business models. Cloud computing represents an opportunity for tremendous cost savings to businesses but also raises security risks. While there has been a great deal of discussion of the privacy risks of storing information "in the cloud," there have not been any legal actions arising from security breaches. Nonetheless, businesses are properly focused on the security aspects of agreements for services in the cloud.

In the context of financial institutions, the Office of the Superintendent of Financial Institutions has released Guideline B-10, setting out its expectations for financial institutions that are considering outsourcing functions such as data storage. Additional precautions could include thorough due diligence of the cloud outsourcing company, legal due diligence regarding the jurisdiction in which the company is located, and careful contract drafting to indemnify the business from security risks related to use of cloud computing.[24] The same economies of scale that make outsourcing of data storage and retention attractive in the first place may be extended to allow the cloud outsourcing company to cost-effectively hire expert security staff; the cloud company may therefore be better suited to bear and insure against the risk of privacy breaches.

Notice Practices

One of the first questions a company faced with a privacy breach must consider is whether it must give notice to the people whose information may have been compromised. Notification practices are still developing. Some legislation requires notification.[25] The federal *Personal Information Protection and Electronic Documents Act*[26] does not currently require notification, but proposed amendments have been introduced that would require notification of "material breaches." Notice is often a useful step in mitigation of any possible damage.[27]

Generally speaking, voluntary notice will have to be weighed against the risk that notice may result in a company being sued even if the breach caused no damage. The unfortunate reality is that notification can lead to litigation, whether

meritorious or not, because even a fear of potential harm is enough to persuade some plaintiffs to sue. On the other hand, businesses sometimes voluntarily decide to notify affected individuals to meet consumer expectations or regulatory best practices[28] and to mitigate any damage.

Is There Any Real Damage?

Not every privacy breach will, or ought to, result in monetary relief. Quite simply, a breach does not necessarily lead to any harm. A number of U.S. lawsuits have been unsuccessful because of the class members' inability to prove "actual harm," and U.S. courts have frequently dismissed class action complaints on this basis.[29]

Remedies sought in privacy class actions vary but often include the cost of credit monitoring, the cost of closing and opening financial accounts, any actual costs associated with identity theft or fraud, and damages for emotional distress.[30] The main focus, however, remains the risk of identity theft,[31] perhaps because an estimated 6.5 per cent of Canadian adults (nearly 1.7 million people) have been affected by identity theft.[32]

U.S. courts have consistently held that the risk of identity theft is too speculative to constitute a compensable injury and that until identity theft actually occurs, there is no actionable wrong. Furthermore, some U.S. courts have found that claims for the costs of protective measures, including credit monitoring, are linked not to actual harm but to the fear of some undefined potential harm and are not recoverable.[33] The cases on this point are "almost uniform in not allowing recovery where there is only a risk of injury and no actual misuse of the stolen electronic data."[34]

The relevance of actual harm has also been recognized in Canada. In *Larose c. Banque Nationale du Canada*,[35] it was only because there was evidence of actual identity theft that the court authorized the class action. The court noted that under Quebec law, the fear of identity theft or fraud does not constitute a harm or an injury in and of itself. Many privacy class actions will be vigorously defended on the basis that the claims seek compensation for pure economic loss, which is often not recoverable in negligence claims.

The range of benefits provided in privacy class action settlements reflects the uncertainty that often surrounds a claim arising from a privacy breach. Settlements have included reimbursement of out-of-pocket expenses incurred after a breach. Certain settlements permit recovery for a reasonable amount of time spent to address the breach or for credit monitoring or identity theft protection measures;[36] others cap the individual recoverable amount.[37]

In the absence of demonstrable economic damages, some courts are moving in the direction of awarding a modest nominal sum as "moral" damages. This has arisen in individual actions. In a recent Federal Court case,[38] the plaintiff sued RBC Royal Bank for unauthorized disclosure of her personal financial information. The plaintiff held a joint RBC Visa card with her husband. The husband was undergoing proceedings related to his divorce from his ex-wife. The ex-wife subpoenaed records relating to all the husband's accounts at the bank, and in response, RBC produced statements for the jointly held Visa card among other records. For this breach of the plaintiff's privacy and the resulting "humiliation," the Federal Court awarded her $2,500.

In *Jones v. Tsige*,[39] the plaintiff was awarded $10,000 in "moral" damages after a Bank of Montreal employee accessed the plaintiff's financial information without authorization 174 times over four years. Emphasizing that the plaintiff suffered no economic damages, the Ontario Court of Appeal nonetheless awarded her $10,000 on the basis that such damages should sometimes be awarded "to vindicate rights or symbolize recognition of their infringement."[40] The court held that such damage awards should be modest and within a conventional range in order to maintain "consistency, predictability, and fairness."[41]

In some settlements arising from cases where there are no economic damages, the rewards are truly nominal. In one U.S. settlement, class plaintiffs who brought a putative action, alleging a technical violation of a statute regulating credit and debit card transactions, were awarded settlement vouchers for $50 off certain store purchases or for a "classy" T-shirt or hoodie.[42] Similarly, in the *TJX Companies* settlement arising out of hackers' unauthorized access to the company's computer network, class plaintiffs were given vouchers for use in TJX stores as well as a bonus of a "One Day Customer Appreciation Sale." In *Parker v. Time Warner Entertainment Co.*,[43] class members were offered the choice of one free month of cable service, two free movies on demand, or a $5 cheque.

In cases arising from business practices that do not lead to demonstrable damages, companies have sometimes agreed to change a specific program or policy to dispel privacy concerns raised by class litigants. These measures may include clarifying terms of use and control over privacy settings associated with a specific program;[44] improving security measures, including full encryption of data;[45] providing an informational "privacy toolkit";[46] completely redrafting a company's privacy policy;[47] or undertaking to retain an independent third party to do a privacy audit of the business.[48]

In response to the number of actions arising from breaches of privacy that did not result in economic harm, some courts have suggested that in such cases, class proceedings may be inappropriate as a matter of policy. In the *Time Warner* settlement approval process, the United States District Court expressed its concern that the combination of consumer protection statutes (containing statutory damages provisions) and class action mechanisms may threaten defendants with liability that is far in excess of any actual harm. Although the court reserved its opinion on whether the *Time Warner* actions should be certified, it also questioned why so much time and labour was being expended to achieve so little.[49]

As the volume of cases continues to expand both north and south of the border, privacy claims will continue to be regularly pursued, and their economic and reputational costs for financial institutions remain to be determined.

Law Still Developing

Privacy law is still at an early stage of development. There is little definitive judicial discussion about the many issues that arise regarding liability, damages, and the time when privacy cases should proceed as class actions. There are also significant differences between the U.S. and Canadian legal landscapes.

Many of the privacy class actions in the United States are based on statutory causes of action that are not available in Canada. For example, the *Electronic Communications Privacy Act* and the *Computer Fraud and Abuse Act* both

provide a cause of action for damages for specific misuses of technology. In Canada, new federal anti-spam legislation, expected to come into force in mid-2013, may impose significant penalties for unsolicited commercial electronic messages, unauthorized installation of computer programs or code, and online fraud.[50]

Another difference between the two jurisdictions is that U.S. law has long recognized invasions of privacy as tortious. However, many commentators have observed that the Canadian common law of privacy has been steadily moving closer to the U.S. model.[51] Ontario law recently took a further step in the U.S. direction in *Tsige*,[52] which adopted the tort of intrusion on seclusion—one of four torts for invasions of privacy set out in the *American Restatement (Second) of Torts*.

Canada, on the other hand, has a sophisticated regulatory regime regarding privacy under *PIPEDA*, which provides a simple administrative process for complaints and appropriate remedies without any need to resort to the courts. Where *PIPEDA* applies, there is a strong argument that class actions are simply not needed, certainly not preferable, and should therefore not be certified. These are among the issues that will be debated in Canadian courts.

[*Editor's note*: **Patrick Flaherty**'s practice focuses on civil litigation with an emphasis on privacy, corporate/commercial, product liability, intellectual property, and class actions.

Molly Reynolds practises civil litigation in a variety of areas, including privacy, corporate/commercial litigation, securities litigation, and class actions.

The authors thank **Frazer House** for his assistance with this article.]

1 *Speevak v. CIBC*, [2010] O.J. No. 770, 2010 ONSC 1128.

2 Class Action Complaint, *Pinero v. Jackson Hewitt Tax Service Inc.*, No. 08-3535 (E.D. Louisiana 2008) [*Jackson Hewitt Tax Service*]; *Cole v. Prairie Centre Credit Union Ltd.*, [2007] S.J. No. 493, 2007 SKQB 330.

3 *MacEachern v. Ford Motor Company of Canada, Ltd. and John Doe Corporation*, filed in the Ontario Superior Court of Justice on January 31, 2013, No. CV-13-18955-CP.

4 "Personally Identifiable Information" has been defined by the Federal Trade Commission as "individually identifiable information from or about an individual including, first and last name; home or other physical address; email address or other online contact information; telephone number; social security number; persistent identifier (i.e. customer number held in a 'cookie' or processor serial number that is combined with other information that identifies an individual) …" as cited in *Valentine v. WideOpen West Finance, LLC*, 2010 U.S. Dist. LEXIS 90566, at para. 25(d).

5 *Jackson v. Canada*, [2005] O.J. No. 2691, 140 A.C.W.S. (3d) 274 (Ont. Sup. Ct.) [*Jackson*].

6 *Waters v. DaimlerChrysler Financial Services Canada Inc.*, [2009] S.J. No. 382, 2009 SKQB 263 [*DaimlerChrysler*].

7 *Rowlands v. Durham Region Health*, [2011] O.J. No. 1864, 2011 ONSC 719.

8 *Rowlands v. Durham Region Health*, [2012] O.J. No. 3191, 2012 ONSC 3948.

9 Jim Bronskill, "We've Lost Personal Information for More Than Half a Million Borrowers: Canada Student Loans," *National Post*, January 11, 2013, <http://news.nationalpost.com/2013/01/11/weve-lost-personal-information-for-more-than-half-a-million-borrowers-canada-student-loans/>.

10 "Human Resources Canada Faces Four Lawsuits over Lost Data," CBC News, January 22, 2013, <http://www.cbc.ca/news/canada/windsor/story/2013/01/22/wdr-human-resources-loans-lost-lawsuits.html>.

11 *Key Steps for Organizations in Responding to Privacy Breaches*, <http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp>.

12 *Ruiz v. Gap, Inc.*, 2010 WL 2170993 (C.A. 9 (Cal.)) [*Ruiz*]; *McLoughlin v. People's United Bank Inc. and Bank of New York Mellon, Inc.*, 2009 U.S. Dist. LEXIS 78065 (D. Conn. 2009) [*McLoughlin*]; *In Re Department of Veterans' Affairs (VA) Data Theft Litigation*, 653 F. Supp. 2d 58 (D.D.C. 2009); Notice of Settlement, Union Pacific Data Breach Class

Action Settlement (D. Nebraska 2007) [Union Pacific]; *Bell v. Acxiom Corporation*, 4:06-cv-00485-WRW (E.D. Ark. 2006) [*Acxiom Corporation*]; *Jackson, supra* note 5; *DaimlerChrysler*, *supra* note 6; *Bordoff v. Gestion d'actifs CIBC Inc./CIBC Asset Management Inc.*, [2010] Q.J. No. 10334, 2010 QCCS 4841.

13 *In re TD Ameritrade Accountholder Litigation*, C-07-2852-VRW (N.D. Cal. 2009); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605 (S.D.N.Y. 2009) [*Emigrant Bank*].

14 *In re Heartland Payment Systems, Inc.*, No. 4:09-MD-2046 (S.D. Tex. 2010) [*Heartland*]; Class Action Complaint, *Ryan v. Delhaize America, Inc. d/b/a Sweetbay, and Hannaford Bros. Co.* (D. Maine 2008) [*Delhaize America*]; *Wong and Churchman v. The TJX Companies Inc.*, filed in the Ontario Court of Justice on January 26, 2007, No. CV070272-00 [*TJX Companies*].

15 [2010] J.Q. no 11510, 2010 QCCS 5385.

16 *Scholes v. Honda Motor Company Ltd.*, filed May 27, 2011, in the Ontario Superior Court of Justice, No. 73038/11.

17 *Heartland*, *supra* note 14.

18 *Silvestri v. Facebook, Inc.*, No. C10-00429 (N.D. Cal. 2010) at 2 [*Silvestri*].

19 [2011] J.Q. no 2323, 2011 QCCS 1118.

20 *Albilia v. Apple Inc.*, [2013] Q.J. No. 6757, 2013 QCCS 2805.

21 Natasha Lomas, "Facebook Users Must Be Allowed to Use Pseudonyms, Says German Privacy Regulator; Real-Name Policy 'Erodes Online Freedoms,'" AOL Inc., December 18, 2012, <http://techcrunch.com/2012/12/18/facebook-users-must-be-allowed-to-use-pseudonyms-says-german-privacy-regulator-real-name-policy-erodes-online-freedoms/>.

22 Selina Koonar, "Canada: Growing Concerns over Online Privacy Lead to Class Action Lawsuits against Instagram, Facebook, and Google," Mondaq Business Briefing, March 15, 2013, <http://www.mondaq.com/canada/x/227178/Data+Protection+Privacy/Growing+Concerns+Over+Online+Privacy+Lead+To+Class+Action+Lawsuits+Against+Instagram+Facebook+And+Google>.

23 Douglas Meal, Mark Szpak, James DeGraw and David McIntosh, "United States: Massachusetts High Court Decision Regarding ZIP Codes Increases Consumer Litigation Risk for Retailers," Mondaq Business Briefing, March 20, 2013, <http://www.mondaq.com/unitedstates/x/227988/Data+Protection+Privacy/Massachusetts+High+Court+Decision+Regarding+ZIP+Codes+Increases+Consumer+Litigation+Risk+for+Retailers>.

24 Office of the Superintendent of Financial Institutions, *Guideline B-10*, <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/guidelines/sound/guidelines/b10_e.pdf>.

25 For example, the Ontario *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule A.

26 S.C. 2000, c. 5.

27 *McLoughlin*, *supra* note 12.

28 Jennifer Stoddart, Privacy Commissioner of Canada, "Privacy and Information and Communications Revolution," May 4, 2011, <http://www.priv.gc.ca/media/sp-d/2011/sp-d_20110504_e.asp>.

29 See, *e.g.*, *Ruiz*, *supra* note 12; *Allison v. Aetna, Inc.*, No. 09-2560 (E.D. Penn. 2010); *McLoughlin*, *supra* note 12; *Randolph v. ING Life Insurance and Annuity Company*, 973 A. 2d 702 at 710 (D.C. Court of Appeals 2009); *Emigrant Bank*, *supra* note 13; *Delhaize America, supra* note 14; and *Acxiom Corporation*, *supra* note 12.

30 *Aetna*, *ibid*. at 2.

31 "Identity Theft Statistics 2010," Identity Theft Labs, February, 18, 2010, <http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/>.

32 Smartswipe, "Canadian Credit Card Theft Stats," March 17, 2009.

33 *Emigrant Bank*, *supra* note 13.

34 *McLoughlin*, *supra* note 12 at 19.

35 [2010] J.Q. no 11510, 2010 QCCS 5385.

36 *Consumer Privacy Cases (Bank of America)* (San Francisco City & County Super. Ct., No. JCCP 4211, 2009); *TJX Companies*, *supra* note 14.

37 Union Pacific, *supra* note 12.

38 *Biron v. RBC Royal Bank*, [2012] F.C.J. No. 1183, 2012 FC 1095.

39 [2012] O.J. No. 148, 2012 ONCA 32 [*Tsige*].

40 *Ibid*. at para. 75.

41 *Ibid*.

42 Under the *Fair and Accurate Credit Transaction Act*, 15 U.S.C. § 1681(g)(1), it is a violation to knowingly print more than five digits of a credit card or debit card with the expiration date on sales receipts at the point of sale.

43 631 F. Supp. 2d 242 (E.D.N.Y. 2009) [*Parker*].

44 *In Re Google Buzz User Privacy Litigation*, No. 5:10-CV-00672-JW (N.D. Cal. 2010).

45 Union Pacific, *supra* note 12.

46 *Consumer Privacy Cases (Bank of America)*, *supra* note 36.

47 *Silvestri*, *supra* note 18.

48 Settlement Agreement, *Palmer v. Sony BMG Music Entertainment*, No. 06-CV-304178CP.

49 *Parker, supra* note 43 at 346–247.

[50] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the *Canadian Radio-television and Telecommunications Commission Act*, the *Competition Act*, the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act*, S.C. 2010, c. 23.

[51] See, for example, Allen M. Linden and Bruce Feldthusen, *Canadian Tort Law*, 9th ed. (Toronto: LexisNexis, 2011), 59; Colin H. H. McNairn and Alexander K. Scott, *Privacy Law in Canada* (Toronto: Butterworths, 2011), ch. 3.

[52] *Supra* note 39.

• BASEL III: AMENDMENTS TO THE LIQUIDITY COVERAGE RATIO
A CANADIAN PERSPECTIVE •

Lisa Mantello and Andrew Lahey
Goodmans LLP

Introduction

On January 6, 2013, the Group of Governors and Heads of Supervision ("GHOS"), the oversight body of the Basel Committee on Banking Supervision ("Basel Committee"), announced that it unanimously endorsed the Basel Committee's amendments to the liquidity coverage ratio ("LCR"), a key component of the Basel III framework.[1] The amendments revise the LCR formulation first announced by the Basel Committee in 2010 ("2010 LCR"). The revised LCR is less rigorous than what the Basel Committee had initially set out and, in many ways, is far less onerous a standard than what financial markets had anticipated.

The LCR standard is aimed at ensuring that banks hold adequate stock of unencumbered high quality liquid assets ("HQLA") to meet liquidity needs for a 30-calendar-day liquidity stress scenario.[2] The GHOS stated that the revised LCR formulation will help prevent central banks from becoming lenders of first resort by requiring banks to hold sufficient levels of liquid assets.[3] The package of amendments is centered on four key elements:

- revisions to the definition of HQLA and net cash outflows
- a timetable for phase-in of the new standard
- a reaffirmation of the usability of the stock of liquid assets in periods of stress, including during the transition period
- an agreement for the Basel Committee to conduct further work on the interaction between the LCR and the provision of central bank facilities

Mervyn King, Chairman of the GHOS, heralded the changes as a very significant achievement, since they provide for a truly global minimum standard for bank liquidity and should enable the global banking system to finance a recovery by allowing liquid assets to be used in times of stress.[4]

Amendments to the Liquidity Coverage Ratio

The Basel Committee developed the Basel III framework in response to the global financial crisis and their recognition that policy weaknesses contributed to the leverage that built up in the financial sector.[5] The LCR, a fundamental element of Basel III, was created specifically to help promote the short-term resilience of banks' liquidity risk profiles.[6] The LCR has two components: (1) the value of the stock of HQLA and

(2) total expected net cash outflows over a 30-calendar-day period.

$$\text{LCR} = \frac{\text{Stock of HQLA}}{\text{Total expected net cash outflows over the next 30 calendar days}}$$

The changes to the definition of the LCR, developed and agreed upon by the Basel Committee, include a broadening of HQLA eligibility and some modifications to the assumed inflow and outflow rates.[7]

The amended standard will require that absent a situation of financial stress, the value of the ratio be no lower than 100 per cent.[8] Basel Committee Chairman Stefan Ingves announced that under the revised LCR, the average LCR for 200 of the world's largest banks would be approximately 125 per cent as of January 2013.[9] This compares to just over 100 per cent under the more rigorous 2010 standard.[10]

The GHOS expects banks to meet the new LCR requirement on an ongoing basis and hold a stock of unencumbered HQLA to defend against potential liquidity stress. However, the GHOS also reaffirmed that during a period of financial stress, banks may use their stock of HQLA and fall below the 100 per cent threshold. National banking supervisors will ultimately be tasked with providing direction on when, to what extent, and for how long banks will be able to use these assets. In Canada, this body is Office of the Superintendent of Financial Institutions ("OSFI"). Canadian banks will be awaiting further guidance from OSFI as implementation of the Basel III requirements draws nearer.

High-Quality Liquid Assets—The Numerator

The numerator of the LCR equation is the stock of HQLA. Under the Basel Committee's standard, banks must hold enough stock of unencumbered HQLA to cover total expected net cash outflows over a 30-day period under a stress scenario. As previously stated, in order to qualify as HQLA, assets should be liquid in markets during periods of stress and, at times, be central bank eligible in central bank operations.[11] The Basel Committee considers assets to be HQLA if they can be easily and immediately converted into cash at little or no loss of value.[12]

The Basel Committee outlined the following fundamental characteristics of HQLA:

- **Low risk:** lower risk assets tend to have higher liquidity. Assets with a low level of legal risk, inflation risk, and in a denomination in a convertible currency with low foreign exchange risk would improve an asset's liquidity.[13]
- **Ease and certainty of valuation:** an asset's liquidity typically increases if market participants can agree on its valuation. Assets with more standardized, homogeneous, and simple structures tend to be more fungible, promoting liquidity.[14]
- **Low correlation with risky assets**: HQLA should not be subject to wrong-way (highly correlated) risk.[15]
- **Listed on a developed and recognized exchange**: being listed increases an asset's transparency.[16]

HQLA comprises Level 1 and Level 2 assets. Level 1 assets can be included without limit, while Level 2 assets can only comprise up to

40 per cent of the stock. One of the significant changes to the 2010 LCR is that national supervisors may include an additional class of assets within Level 2, provided that these Level 2B assets comprise no more than 15 per cent of the total stock of HQLA.[17] They must also be included within the overall 40 per cent limit of Level 2 assets.

Level 1 Assets

Level 1 assets remain the same under the revised LCR and generally include cash, central bank reserves,[18] and certain marketable securities backed by sovereigns and central banks. These assets are typically the most liquid and of the highest quality.[19] Level 1 assets can comprise an unlimited share of the pool and are given their full value under the LCR. However, national bank supervisors may require haircuts for Level 1 securities, based on—among other things—their duration and credit and liquidity risk. For purposes of the LCR, the Basel Committee stated that Level 1 assets in the stock of HQLA should be measured at an amount no greater than their current market value.[20]

Another example of an important amendment to the 2010 LCR surrounds the clarification of the language and confirmation that supervisors have national discretion to include or exclude required central bank reserves (as well as overnight and certain term deposits) as HQLA as they consider appropriate.[21] With this in mind, local supervisors should discuss with the relevant central banks the extent to which central bank reserves are able to be drawn down in times of stress, and whether this is in line with their policies.[22]

Level 2 Assets Generally

Level 2 assets (comprising Level 2A assets and any Level 2B assets permitted by national supervisors) can be included in the stock of HQLA, subject to the requirement that they comprise no more than 40 per cent of the overall stock after applying haircuts.[23]

Level 2A Assets

A 15 per cent haircut is applied to the current market value of each Level 2A asset held in the stock of HQLA. Level 2A assets are those that formed part of the Level 2 assets for purposes of the 2010 LCR and include certain liquid marketable securities guaranteed by sovereigns, central banks, or multilateral development banks that satisfy various prescribed conditions (*i.e.*, must be reliable sources of liquidity in the market even during stressed market conditions), covered bonds, and corporate debt securities that satisfy various conditions (*i.e.*, rating requirements).[24]

Level 2B Assets

Level 2B assets may be included at the discretion of national authorities but are given a larger haircut than Level 2A assets. Level 2B assets include lower rated corporate debt securities, residential mortgage-backed securities ("RMBS"), and common equity shares that meet certain conditions.[25] Level 2B assets are limited to no more than 15 per cent of a bank's total stock of HQLA for purposes of the revised LCR.

(1) RMBS

RMBS that satisfy certain prescribed conditions may be included in Level 2B assets subject to a 25 per cent haircut. This 25 per cent haircut rate for certain RMBS represents a notable amendment to the 2010 LCR. One condition that RMBS must satisfy is that they must not have been issued by, and the underlying assets must not have been originated by, the bank itself or any of its affiliated entities. RMBS must also have a long-term credit rating of AA or higher from a recognized

external credit assessment institution or, in the absence of a long-term rating, a short-term rating equivalent in quality. Additionally, RMBS must have a proven record as a reliable source of liquidity even during stressed market conditions.[26]

Another condition is that, at issuance, the underlying mortgages must be "full recourse" loans and have, on average, a maximum loan-to-value ratio of 80 per cent.[27] In Canada, mortgages are "full recourse" loans in almost all of the provinces,[28] and borrowers remain responsible for the full obligation of their mortgages even in cases of enforcement on the mortgage.[29] On average, Canadian homeowners have loan-to-value ratios of roughly 55 per cent of total home value,[30] which is less than in the United States.[31] These facts suggest that in the Canadian marketplace, at the very least, some RMBS would satisfy this LCR condition and be included in the Level 2B asset category.

(2) Corporate Debt Securities

Corporate debt securities (including commercial paper) may also be included in Level 2B subject to a 50 per cent haircut and certain specified conditions. Once again, this haircut rate represents a change to the 2010 LCR. In order to be included as a Level 2B asset, the corporate debt securities must not have been issued by a financial institution or any affiliated entities. The corporate debt securities must either (1) have a long-term credit rating between A+ and BBB- from a recognized external credit assessment institution or—in the absence of a long-term rating—a short-term rating equivalent in quality or (2) not have a credit assessment by a recognized external credit assessment institution and be internally rated as having a probability of default corresponding to a credit rating between A+ and BBB-. The corporate debt securities must additionally be traded in large, deep, and active repo or cash markets characterized by low levels of concentration. Finally, even during periods of stress, the corporate debt securities must have a proven record as reliable sources of liquidity in the markets.[32]

Over the past several years, corporate debt included in Bank of America Merrill Lynch's Canadian Corporate Index has had an average rating of A2—one level higher than the A3 average ranking of the securities in the U.S. Corporate Master Index.[33] Moreover, with the exception of 2012, Canadian corporate bonds outperformed Canadian federal and provincial notes every year since 2008.[34] This suggests that a large number of Canadian corporate debt securities will be eligible for inclusion in a bank's stock of HQLA.

(3) Common Equity Shares

Common equity shares may also be included in Level 2B subject to a 50 per cent haircut and certain prescribed conditions. Many of the conditions match those required for corporate debt securities. For example, much like with corporate debt securities, the common equity shares must not have been issued by a financial institution or any affiliated entities. These shares must also be exchange traded and centrally cleared, and they must trade in large, deep, and active repo or cash markets characterized by low levels of concentration. Additionally, the common equity shares must also have a proven record as a reliable source of liquidity in the markets even during periods of stress.[35] Relative to other equity markets in the developed world, the continuing strong

fundamentals of the Canadian equity market would arguably make Canadian common equity shares a relatively reliable source of liquidity for Canadian banks.[36] This suggests that Canadian common equity shares could constitute a large proportion of Level 2B assets under the LCR.[37]

In many ways, the amendments to the 2010 LCR are a balance between the benefits of greater diversification of the liquidity pool and the costs associated with the inclusion of slightly lower quality assets.[38]

Total Expected Net Cash Outflows—The Denominator

The denominator of the LCR equation is total net cash outflows. Total net cash outflows are defined for purposes of the LCR as

Total expected net cash outflows over the next 30 calendar days
=
Total expected cash outflows
–
the lesser of
(1) Total expected cash inflows over the next 30 calendar days and
(2) Seventy-five per cent of total expected cash outflows over the next 30 calendar days

To assess the potential total expected cash outflows, the LCR assumes that a bank will experience certain liquidity pressures during a period of stress. The types of liquidity pressures assumed include—but are not limited to—(1) withdrawals by customers from retail and wholesale deposit accounts, (2) the need to post additional collateral in transactions as a result of a downgrade in the bank's external credit rating, and (3) the need to post additional collateral in derivative transactions as a result of changes in the market value of collateral posted.

Total expected cash outflows are calculated by multiplying the outstanding balances of various categories of liabilities and off-balance sheet commitments by the rates at which they are expected to "run-off" or be drawn down. The "run-off" rate in this context refers to the amount of funding that would be maturing in the 30-day window that would not rollover (*i.e.*, deposit withdrawals). The LCR assigns various run-off rates to different categories of assets.

Total expected cash inflows are calculated by multiplying the outstanding balances of various categories of contractual receivables by the rates at which they are expected to flow in. Total cash inflows are subject to an aggregate limit of 75 per cent of total expected cash outflows, thereby guaranteeing a minimum level of HQLA holdings.[39]

Cash Outflows

There are specific requirements for cash outflows in connection with the LCR. While the following discussion is not exhaustive, certain notable elements have been explored in greater detail.

(1) Retail Deposits

Retail deposits subject to the LCR include demand deposits and term deposits. For purposes of the LCR, retail deposits are divided into "stable" and "less stable" portions of funds with run-off rates of 3 per cent for stable deposits that are insured under a scheme that meets certain requirements,[40] 5 per cent for deposits that are stable but are not covered by a qualifying insurance plan, and 10 per cent for less stable deposits.

(2) Wholesale Deposits

Wholesale deposits are deposits by legal entities, sole proprietorships, or partnerships. Generally

speaking, deposits provided by small business customers will assume a run-off rate between 5 per cent and 10 per cent and higher in certain instances. Deposits by wholesale customers with a specific operational relationship with a bank previously received a run-off rate of 25 per cent under the 2010 LCR. The amended LCR allows a run-off rate of 5 per cent for these operational deposits by wholesale customers for the portion of stable deposits insured in a qualifying regime.

Under the 2010 LCR, the deposits of sovereigns, central banks, public sector entities, non-financial corporate and multilateral development banks received an assumed run-off rate of 75 per cent in a stress scenario. The amended LCR allows a 20 per cent outflow rate if the amount of such a deposit is fully insured by a program that meets certain requirements and a 40 per cent outflow rate otherwise.

(3) Derivatives Cash Outflows

Pursuant to the LCR, 100 per cent of the sum of all net cash outflows on derivatives transactions will be included in the calculation of total net cash outflows. Cash flows may be calculated on a net basis by a counterparty where a valid master netting agreement is in place.

The introduction of increased liquidity requirements related to a bank's downgrade trigger in its derivatives and a standardized approach for liquidity risk related to market value changes in collateral posted on derivatives transactions[41] are notable amendments to the 2010 LCR.

(A) Liquidity Needs Related to Downgrade Triggers

It is common in derivative transactions to have clauses that require the posting of additional collateral, drawdown of contingent facilities, or early repayment of existing liabilities upon the bank's downgrade by a recognized credit-rating agency. For purposes of the LCR, 100 per cent of the amount of collateral that would be posted for, or contractual cash outflows associated with any ratings downgrade (up to and including a 3-notch downgrade) of the bank, must be included in the calculation of net cash outflows.

(B) Liquidity Needs Related to Valuation Changes in Posted Collateral

In collateralized derivative transactions, counterparties are typically required to secure the mark-to-market valuation of their positions. When Level 1 assets are posted as collateral, there is no requirement for additional stock of HQLA to be reserved for potential valuations changes in the collateral posted.[42]

(4) Cash Outflows Related to Asset-Backed Securities, Covered Bonds, and Other Structured Financing Instruments

The Basel Committee recommends that asset-backed securities, covered bonds, or other structured financing instruments issued by the bank itself assume a 100 per cent outflow of a transaction that matures within the 30-day period, as the stress scenario assumes that the refinancing market will not exist.

Cash Inflows

When assessing available cash inflows, the Basel Committee recommends that banks only include contractual inflows (including interest) from outstanding exposures that are fully performing and for which the bank does not anticipate defaults within 30 days. Certain notable requirements for cash inflows are summarized in the following section.

(1) Secured Lending, including Reverse Repos and Securities Borrowing

The Basel Committee recommends that banks assume that maturing reverse repurchase or securities borrowing agreements secured by Level 1 assets will be rolled over and not give rise to any cash inflows in a stress scenario. Collateralized loans extended to customers for the purpose of taking leveraged trading positions (*i.e.*, margin loans) are also considered a form of secured lending under the LCR; however, banks may recognize no more than 50 per cent of contractual inflows from these types of loans made against non-HQLA collateral.[43]

(2) Committed Facilities

The Basel Committee recommends that banks assume that no facilities that they hold at other institutions for their own purposes be drawn upon in a stress scenario. These facilities will receive a 0 per cent inflow rate for purposes of the LCR.

(3) Other Inflows by Counterparties

For all other types of transactions, either secured or unsecured, the inflow rate will be determined by counterparty; however, limits on contractual inflows by counterparty type will be applied under the LCR. A net inflow value of 50 per cent of the contractual amount will be applied to loans from retail and small businesses. With respect to wholesale inflows, an inflow value of 100 per cent will be applied for financial institution and central bank counterparties; 50 per cent, for non-financial wholesale counterparties. Inflows from securities—not included in the stock of HQLA—maturing within 30 days should be treated with an inflow of 100 per cent. Deposits held at other financial institutions for operational purposes, and deposits held at centralized institutions in a co-operative banking network will both receive a 0 per cent inflow rate.

Phase-in Arrangements

In endorsing the LCR amendments, the GHOS also agreed that the LCR should be subject to phase-in arrangements that best align with those that apply to the Basel III capital adequacy requirements. The LCR will therefore be introduced as planned on January 1, 2015; however, the minimum requirement will begin at 60 per cent, rising in annual increments of 10 per cent to reach 100 per cent by January 1, 2019 (as identified in the table below).

	Jan. 1, 2015	Jan. 1, 2016	Jan. 1, 2017	Jan. 1, 2018	Jan. 1, 2019
Minimum LCR	60%	70%	80%	90%	100%

Implementation

As previously stated, in Canada, OSFI is the competent national authority for implementation of Basel III and has recently joined the list of international regulators that have met their commitment to implement Basel III in their domestic regulatory frameworks. OSFI states that it is confident that over time these initiatives will help foster public confidence in the implementation of Basel III and demonstrate that the promises made by G20 countries, such as Canada, are being matched by actions. Much still needs to be accomplished, but OSFI has stated publicly that the end result will be a safer, more resilient financial system in Canada.[44]

With respect to the LCR, the Assistant Superintendent of OSFI was recently quoted as saying that OSFI will need to fully examine how its existing liquidity monitoring tools should be used in conjunction with the new international

standards.[45] OSFI has made concerted efforts to ensure that they not only accelerate the implementation of Basel III but also do so in a manner that makes sense for Canadian institutions.

Much like in other jurisdictions, the changes to the LCR are anticipated to be well received by Canadian banks not only for the reason that the standard has been eased considerably but also because they will now have more time to comply with the rule.

[*Editor's note*: **Lisa Mantello** is a partner in the Goodmans LLP finance group. She practises in all areas of financial services with a particular focus on structured finance and lending.

Andrew Lahey is an associate at Goodmans LLP. He practises in the areas of corporate law, mergers and acquisitions, securities law, and banking and finance law.]

---

1 The Basel Committee on Banking Supervision's amendments to the liquidity coverage ratio are described in greater detail in the official publication entitled *The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools*. Excerpts of the official publication have been reproduced for purposes of this article. See Basel Committee on Banking Supervision, *Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools*, Bank for International Settlement (January 2013), <http://www.bis.org/publ/bcbs238.pdf>.

2 Bank for International Settlement, *Annex 1: Summary Description of the LCR*, <http://www.bis.org/press/p130106a.pdf>.

3 Bank for International Settlement, *Press Release: Group of Governors and Heads of Supervision Endorses Revised Liquidity Standard for Banks*, <http://www.bis.org/press/p130106.pdf>.

4 *Ibid.*

5 Stefan Ingves, *From Ideas to Implementation*, Bank for International Settlement, <http://www.bis.org/review/r130124a.pdf>.

6 *Supra* note 2.

7 *Supra* note 3.

8 In Annex 1 to the press release announcing the amendments dated January 6, 2013, the GHOS stated that the 100 per cent threshold will be the minimum requirement, after the phase-in arrangements are complete, absent a period of financial stress. Additionally, references to 100 per cent may be adjusted for any phase-in arrangements in force at a particular time.

9 *Supra* note 5.

10 *Ibid.* It was also noted that this does not mean that all banks are ready to meet the standard. Even though the industry average is well above the minimum, the Basel Committee's estimation suggests that approximately one-quarter of the banks used as samples could still have an LCR below 100 per cent taking the latest policy changes into account.

11 *Supra* note 1.

12 *Ibid*.

13 *Ibid*.

14 *Ibid*. It is noteworthy that the Basel Committee commented that HQLA should have a pricing formula that is easy to calculate with publicly available inputs. They note that this would exclude structured or exotic products from HQLA.

15 *Ibid*.

16 *Ibid*.

17 *Ibid.*

18 Central bank reserves would, for example, include banks' overnight deposits with the central bank and term deposits with the central bank that (1) are explicitly and continually repayable on notice from the depositing bank or (2) constitute a loan against which the bank can borrow on a term basis or on an overnight but automatically renewable basis (only where the bank has an existing deposit with the relevant central bank).

19 *Supra* note 2.

20 *Supra* note 1.

21 Bank for International Settlement, *Annex 2: Complete Set of Agreed Changes to the Formulation of the Liquidity Coverage Ratio Published in December 2010*, <http://www.bis.org/press/p130106b.pdf>.

22 *Supra* note 1.

23 *Ibid.*

24 *Supra* note 2.

25 *Ibid*.

26 Compared to the United States, Canadian mortgage products tend to be lower risk, as the rate of United States mortgage arrears is more than ten times higher than in Canada. See Canadian Bankers Association, *Canada's Strong Banking System: Benefitting Canadians*, <http://cba.stage6.industrialmedia.ca/contents/files/backgrounders/bkg_cdnbankingsystem_en.pdf>.

27 *Supra* note 1.

[28] An exception to this is that certain types of uninsured mortgages in Alberta and Saskatchewan are non-recourse.

[29] Canada Mortgage and Housing Corporation, *Housing Finance*, <http://www.cmhc.ca/en/corp/about/cahoob/upload/Chapter_2_EN_dec21_w.pdf>.

[30] Canada Mortgage and Housing Corporation, *CMHC Mortgage Loan Insurance at a Glance*, <http://www.cmhc-schl.gc.ca/en/corp/nero/jufa/jufa_033.cfm>.

[31] *Supra* note 26.

[32] *Supra* note 1.

[33] Frederic Tomesco, "CIBC Sees Corporate Bonds Regaining Dominance," *Financial Post*, January 11, 2012, <http://business.financialpost.com/2012/01/11/cibc-sees-corporate-bonds-regaining-dominance/>.

[34] *Ibid.*

[35] *Supra* note 1.

[36] David Milstead, "Canadian Equity Market Beats Emerging Nations," *Globe and Mail*, March 7, 2011, <http://www.theglobeandmail.com/globe-investor/investment-ideas/canadian-equity-market-beats-emerging-nations/article4265974/>.

[37] *National Post*, "Canadian Equity Market 'Never More Attractive,'" *Financial Post*, <http://www.financialpost.com/scripts/story.html?id=cc93e380-b33b-4cae-83c2-ca1007b41c3f&k=22832>.

[38] *Supra* note 5.

[39] *Supra* note 1.

[40] In Canada, the Canadian Deposit Insurance Corporation ("CDIC") insures Canadians' deposits held at Canadian banks (and other financial institutions) for up to $100,000. CDIC members will need to comply with the Basel III liquidity coverage ratio requirements by 2015. See Canada Deposit Insurance Corporation, *Management's Discussion and Analysis*, <http://www.cdic.ca/CDIC/FinRpts/Documents/AR2012/AR2012_P1.pdf>. In order to receive a run-off rate of 3 per cent, the following additional criteria for deposit insurance schemes must be met:

- the insurance scheme must be based on a system of prefunding via the periodic collection of levies on banks with insured deposits
- the scheme must have adequate means of ensuring ready access to additional funding in the event of a large call on its reserves (i.e., an explicit and legally binding guarantee from the government or a standing authority to borrow from the government
- access to insured deposits must be available to depositors in a short period once the deposit insurance scheme is triggered

[41] *Supra* note 20.

[42] When mark-to-market exposures are collateralized with lesser forms of collateral than Level 1 assets, 20 per cent of the value of all such posted collateral, net of collateral received on a counterparty basis (provided that the collateral received is not subject to restrictions on reuse or rehypothecation) will be added to the stock of required HQLA by the bank posting the collateral.

[43] *Ibid.*

[44] Office of the Superintendent of Financial Institutions Canada, *Promoting a Safe and Sound Financial System: Lessons from the Goose that Laid the Golden Egg*, <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/speeches/mz20121121_e.pdf>.

[45] Office of the Superintendent of Financial Institutions Canada, *Regulatory Resolutions for 2013*, <http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/speeches/mz20130108_e.pdf>.

INVITATION TO OUR READERS

Have you written an article on a current issue that you think would be appropriate for *National Banking Law Review*?

Do you have any suggestions for topics you would like to see featured in future issues of *National Banking Law Review*?

If so, please feel free to contact us at nblr@lexisnexis.ca

The *National Banking Law Review* is published six times per year by LexisNexis Canada Inc.
This issue is cited as 32 Nat. B.L. Rev.

You can contact the LexisNexis Editor at:

Telephone (905) 479-2665, ext. 308 Toll-Free Telephone 1-800-668-6481
Fax (905) 479-2826 Toll-Free Fax: 1-800-461-3275
Internet e-mail: nblr@lexisnexis.ca

Price: $425 for six issues and annual index. Binder available at $20 upon request.
$495 for Print & PDF

ISBN 0-409-91076-7 ISSN 0822-1081
ISBN 0-433-44389-8 (Print & PDF)
ISBN 0-433-44684-6 (PDF)

The Journal is indexed in the *Index of Canadian Periodical Literature*
and in *the Index to Canadian Legal Literature*.
Publications Mail Registration No. 180858