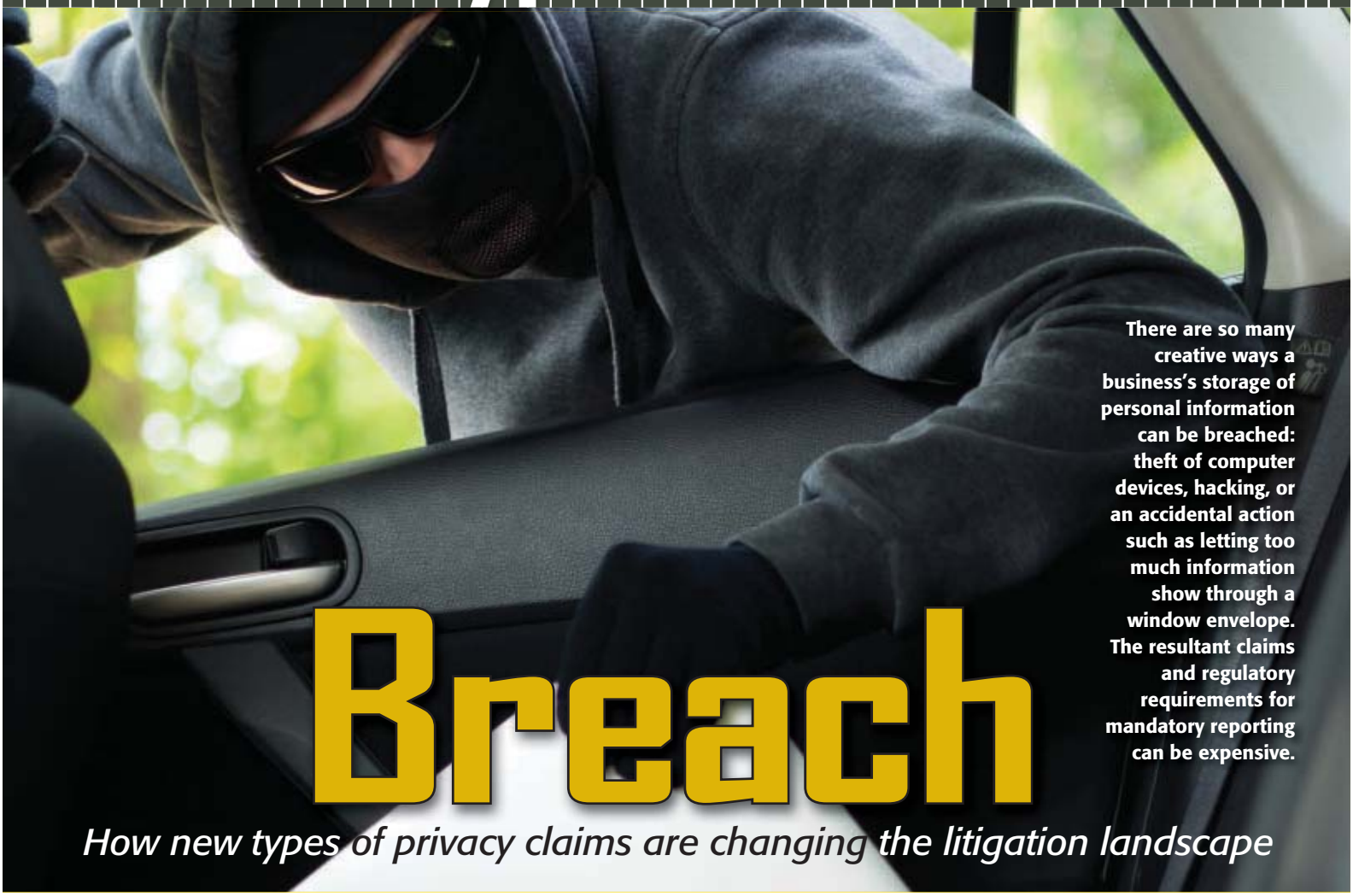

Breach

How new types of privacy claims are changing the litigation landscape

There are so many creative ways a business's storage of personal information can be breached: theft of computer devices, hacking, or an accidental action such as letting too much information show through a window envelope. The resultant claims and regulatory requirements for mandatory reporting can be expensive.

By Daniel Reid

Advances in technology have fundamentally altered the way people and corporations collect, store and disclose customer information. An app on a smartphone or wearable device can track a user's location history, financial information and, increasingly, personal health information such as diet, exercise and sleep habits. A single laptop can contain the business or health records of thousands of customers. As the 2015 hack of the online dating website Ashley Madison and the subsequent release of its user information demonstrate, a company's servers can contain the private data of millions.

The proliferation of electronic personal information and changes to federal and provincial law has resulted in an increase in litigation for "breach of privacy"[1] arising out of unauthorized use and disclosure of "personal information".[2] While awards to individual plaintiffs in data breach cases are typically in the range of several hundred to several thousand dollars, class action lawsuits could result in awards in the hundreds of millions of dollars. Mandatory breach notification laws, as well as new regulatory penalties for failure to comply with privacy legislation, further increase the potential costs to companies arising out of a privacy breach.

Depending on the nature of the privacy breach, there may or may not be insurance coverage to protect a company or its employees from these costs. It is no longer enough for a company to assume the privacy provisions in the standard Commercial General Liability Policy are sufficient to protect it in the event of a privacy breach. In this article, we review the types of claims and expenses

IBABC HyperArticle™ Brokers can earn a CE technical credit with this article: 1. Go to *www.thelearningportal.ca/ibabc/*. 2. Review the article and the supplemental information. 3. Successfully complete the quiz. Cost: One-year subscription and access to all HyperArticles $69.00. New HyperArticles will be added throughout the year. This article is ideal for all brokers. Licensees can earn 1 CE credit.

that can occur as a result of privacy breaches, potential changes in B.C. that could result in more of these claims being commenced, and highlight coverage issues that the courts will be addressing in the coming years.

Types of breaches – theft, accidental or deliberate

In recent years a number of high-profile lawsuits have resulted from the actions of third parties, such as theft or hacking, in which customer information is maliciously obtained. For example, in 2011, hackers accessed the personal information of tens of millions of users of Sony's online PlayStation Network gaming service, including names, addresses, birth dates and potentially financial information.[3] In 2013, criminals illegally obtained the payment-card information of up to 40 million customers of the American retailer Target, as well as their names, mailing addresses, email addresses and phone numbers.[4] In the 2015 Ashley Madison breach, hackers breached the databases of a Canadian-based online dating website and gained access to up to 37 million user profiles, threatening to release personal information if the site was not immediately shut down.[5] Each of these breaches resulted in lawsuits – in the case of Ashley Madison, a massive $760-million class action lawsuit on behalf of all residents of Canada who subscribed to the website.[6]

Privacy breaches can also occur as the result of physical theft, such as an employee laptop or phone with customer information being stolen. However, many privacy breaches result from the deeds of internal actors, such as deliberate actions (snooping) by employees. By way of example, in the 2012 *Jones v. Tsige* case, the Ontario Court of Appeal recognized the right of Ontarians to bring a civil action for invasion of personal privacy, following a bank employee deliberately and repeatedly accessing the private banking records of her spouse's ex-wife. A recent review of health authority privacy breach management by the B.C. Privacy Commissioner expressed concern about the "number of occurrences of inappropriate access to electronic heath records by health authority employees and deliberate disclosures via social media and through personal mobile devices like cellular telephones."[7]

Employee errors can also result in legal liability for privacy breaches – in April 2015, a British Columbia court awarded $2,000 in damages to a plaintiff who sued her bank for breach of privacy, alleging the bank mistakenly mailed her financial information to her ex-husband and provided inaccurate information to credit reporting bureaus.[8] In July 2015, the Federal Court certified a class action lawsuit against Health Canada for mailing correspondence to authorized medical marijuana users; the envelope used by Health Canada made visible the name of the individual and the name of the medical marijuana program.[9]

It is not just theft, mistakes or unauthorized actions that result in privacy lawsuits; there have been a number of recent class action lawsuits commenced in Canada alleging the deliberate policies and procedures of companies and organizations resulted in breaches of privacy. For example, in April 2015, a $750-million national class action lawsuit was filed against Bell Canada, related to unauthorized tracking of customers' cellphone internet usage. The suit claims Bell tracked, collected and sold customers' sensitive account and internet browsing information to advertisers.[10]

Types of legal actions

Privacy breaches can occur in a number of ways – deliberate theft by third parties, errors or omissions by employees, or as a result of policies and procedures employed by an organization. Lawsuits related to privacy breaches can be brought on a number of bases – in recent years plaintiffs have advanced a number of unique and creative types of privacy-based claims, including: claims in tort (breach of privacy or negligence), claims in contract, and claims for "waiver of tort." Such claims can be advanced in Canada even if the plaintiff has not suffered any actual damage. In addition, mandatory reporting requirements (more on this later) could result in companies and organizations incurring significant costs to notify all individuals affected of a breach. The potential costs of such claims and reporting requirements are massive, particularly when coupled with class action lawsuits. Let's look at these three types of privacy-based claims:

1. Claims in tort

The 2012 *Jones* case, mentioned earlier, has been a catalyst for an increase in breach-of-privacy tort claims in Canada. In the *Jones* case, the Ontario Court of Appeal recognized the right to sue for the common-law tort of "intrusion upon seclusion," a tort which had previously been recognized in a number of American states but had not been adopted by the common law in Canada. In *Jones*, the Ontario Court of Appeal held that a civil action can be brought where a defendant "intentionally, and without lawful justification," invades the plaintiff's private affairs or concerns and where a reasonable person would regard the invasion as "highly offensive." Importantly, the court held that economic damage was not a required element of the tort – the plaintiff in *Jones* recovered $10,000, despite no evidence of actual damage. Prior to the *Jones* case, Ontario did not recognize an individual's right to claim for breach of privacy under the common law.

At the federal level, the class action against Health Canada for sending envelopes with the names of individuals and "Marijuana Medical Access Program" was allowed to proceed on the basis of the novel tort of "publicity given to private life."[11] It is likely that, in the coming years, other jurisdictions in Canada

[1] The Office of the Privacy Commissioner of Canada defines privacy breach as the result of an unauthorized access to, or collection, use or disclosure of, personal information. Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA), or similar provincial privacy legislation.

[2] Section 2(1) of the PIPEDA states that "personal information" means "information about an identifiable individual."

[3] http://www.pcworld.com/article/226802/playstation_network_hack_timeline.html

[4] https://corporate.target.com/about/shopping-experience/payment-card-issue-faq

[5] https://en.wikipedia.org/wiki/Ashley_Madison#Data_breach, see also http://www.insurancebusiness.ca/news/ashley-madison-hack-offers-valuable-lesson-on-coverage-gap-193458.aspx

[6] https://www.charneylawyers.com/Charney/ashleymadisonclassaction.php

[7] https://www.oipc.bc.ca/media/16779/examination-of-british-columbia-health-authority-privacy-breach-management.pdf, at page 21

[8] *Albayate v. Bank of Montreal*, 2015 BCSC 695 http://www.canlii.org/en/bc/bcsc/doc/2015/2015bcsc695/2015bcsc695.pdf

[9] *John Doe v. Canada*, 2015 FC 916 http://www.canlii.org/en/ca/fct/doc/2015/2015fc916/2015fc916.pdf

[10] https://www.bellmobilityprivacybreach.com/

[11] http://lernersclassactionplaintiff.ca/blog/post/novel-privacy-tort-recognized-in-certification-of-marihuana-medical-access-plan-class-action?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original#_ftn1

will substantially adopt the common-law torts recognized by the Ontario and federal courts, or recognize new types of claims based on an individual's right to privacy.

While some provinces do not yet recognize a common-law right to sue for the tort of "breach of privacy," Alberta, British Columbia and Quebec already have privacy legislation that includes the right of private individuals to sue for breach of privacy. In British Columbia, the *Privacy Act*, RSBC 1996, c. 373 states:

(1) It is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another.

(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.

In practice, the common-law and statute-based torts are very similar – both require an intentional or willful breach of privacy that is to be interpreted "contextually" by the courts, both in relation to the nature of the breach and any lawful justification provided by the parties.

2. Claims in contract

In addition to claiming in tort, a number of recent privacy cases have also involved contractual claims, alleging that by way of contract (such as an employment contract or privacy policy), the defendants agreed to use or protect private information in a certain way. Recent case law suggests that a party may, by the mere act of publishing a privacy policy or privacy code online, contractually bind itself to handling personal information in a manner consistent with the policy.

In the recent British Columbia case of *Albayate v. Bank of Montreal*, 2015 BCSC 695, the claimant sued in tort, alleging that her bank sent her ex-husband her private financial information, and in contract, alleging that the bank failed to correct her address in communications to credit bureaus, in violation of the bank's own privacy code. The bank's privacy code contained the following statement:

"This Privacy Code outlines our commitment to you and is designed to comply with the applicable Privacy legislation in Canada, which incorporates the following (10) principles...

Be Accurate

We are committed to maintaining the accuracy of your personal information and ensuring that it is complete and up-to-date. If you discover inaccuracies in our data, or your personal information changes, please notify the branch or office where you do business immediately, so that we can make the necessary changes. When required, we will make our best efforts to advise others of any important amendments to your personal information that we may have released to them..."

The plaintiff's claim in tort failed, as although there was a breach resulting from her financial information being sent to her ex-husband, "the breach did not result in any unauthorized disclosure because Mr. Albayate did not open the mail." However, the claim in contract was successful, with the trial judge finding "the bank was in breach of its privacy policy, which formed part of its contract with Ms. Albayate, in providing inaccurate information to the credit bureaus and by not correcting the inaccurate information when it became aware the address had been changed in its computer system without her authorization."

In future, companies will have to ensure that they are not inadvertently opening the door to litigation by promising to handle personal information in a particular manner and then failing to do so.

While the plaintiff was only awarded $2,000 in damages for this nominal breach, the potential for a company to be sued under contract on the basis of its privacy policy is potentially quite significant. In the future, companies will have to ensure that they are not inadvertently opening the door to litigation by promising to handle personal information in a particular manner and then failing to meet these self-imposed obligations.

3. Waiver of tort

A third type of claim arising out of privacy breaches is "waiver of tort," in which a party sues on the basis that the defendant has earned profits because of wrongful conduct in relation to personal information. Wrongful conduct can potentially include not taking adequate steps to protect personal information, or deliberate actions such as selling private information to advertisers.

In December 2014, the Ontario Superior Court of Justice upheld the certification of a claim against a bank that included a claim for waiver of tort, relating to the unauthorized access of customer information by a bank employee (*Michael Evans and Crystal Evans v. The Bank of Nova Scotia and Richard Wilson*, 2014 ONSC 7249). In this case, a bank employee accessed private and confidential financial information of bank customers, without authorization, and then passed this information on to his girlfriend, who then provided the information to third parties for fraudulent purposes. The plaintiffs successfully argued that their claim in waiver in tort against the bank could proceed on the basis that the bank's business model did not adequately supervise its employees to ensure that customers' confidential information remained private, and that the bank profited from the savings resulting from not implementing a supervision system.[12]

The recently started $750-million class action lawsuit against Bell Canada also claims in "waiver of tort," alleging that Bell Canada improperly profited by deliberately using customer account and network-usage information to generate marketing reports that were then sold to advertisers. The development of this tort in relation to claims for breach of privacy is still in its infancy, but its emergence muddies the already-complicated legal waters surrounding breach of privacy claims.

Class actions

While it has become easier in Canada to sue for privacy breaches, damages for individual plaintiffs have typically been quite low. In the Ontario case of *Jones*, the court put a general cap on individual damages for breaches of privacy of $20,000. As a result, it may not always be economical for an individual plaintiff to sue for breach of privacy, particularly in jurisdictions like British Columbia that preclude the bringing of a claim pursuant to the *Privacy Act* in small claims court.

While individual damages may be low, the potential cost to companies where there is a class of affected individuals could be astronomical. There has been an increase in class action lawsuits arising out of privacy breaches in Canada,

including claims in which the potential class of plaintiffs could number in the millions.

By way of example, in a case filed in 2012 in B.C., a plaintiff commenced a potential class action claim against Google[13] on behalf of "all persons in the province of British Columbia who have sent email to a Gmail account," alleging that Google scanned Gmail users' email for the purpose of providing advertising service (a similar action was denied class certification in the United States in March 2014).[14]

Similarly, in 2014 the B.C. Supreme Court certified a class action on behalf of all B.C. Facebook users, in which the plaintiffs alleged that Facebook's use of the names and images of Facebook users in B.C. in advertisements was a breach of the *Privacy Act* of B.C.[15] The B.C. Court of Appeal subsequently held that the lawsuit could not proceed in British Columbia, as Facebook's terms of use contained a forum selection clause under which Facebook users agreed to bring any legal proceedings in Santa Clara, California.[16]

The recent cases against Bell Canada and Ashley Madison, both of which seek in excess of $700 million, are class actions, and are brought on behalf of a large group of plaintiffs potentially affected by the alleged privacy breach. As more people learn of privacy breaches and their potential legal rights, the number of large claims on behalf of groups of plaintiffs is bound to increase.

Mandatory reporting and federal penalties

A further complicating factor is the requirement in some jurisdictions to notify affected users of privacy breaches. Unlike other Canadian jurisdictions, British Columbia currently lacks a "mandatory reporting" requirement in its privacy legislation. That means that it is up to public and private bodies to "voluntarily" disclose privacy breaches to the Office of the Privacy Commissioner of British Columbia and to affected individuals.

This is something B.C.'s Privacy Commissioner Elizabeth Denham has said should change. She has been quoted as saying that citizens "expect to be told when their information has been compromised," and in February 2015, a special legislative committee recommended that B.C. legislation be amended to require companies to notify the Office of the Privacy Commissioner and all affected individuals where there is "a real risk of significant harm" as a result of a breach.[17]

At the federal level, a section of the *Digital Privacy Act* (Bill S-4), which was passed on June 18, 2015, but has yet to come into force, requires organizations to notify affected individuals and the

Continued on page 36 >

[12] http://www.canlii.org/en/on/onsc/doc/2014/2014onsc7249/2014onsc7249.pdf
[13] http://www.canlii.org/en/bc/bcsc/doc/2013/2013bcsc681/2013bcsc681.pdf http://cauce.typepad.com/files/plimmerv.google.pdf
[14] http://www.reuters.com/article/us-google-gmail-lawsuit-idUSBREA2I13G20140319
[15] *Douez v. Facebook*, Inc., 2014 BCSC 953
[16] *Douez v. Facebook*, Inc., 2015 BCCA 279
[17] http://www.timescolonist.com/news/local/watchdog-urges-compulsory-reporting-of-b-c-privacy-breaches-1.2033472

Breach

< *Continued from page 9*

Privacy Commissioner of Canada where there is a reasonable belief that the breach creates a "real risk of significant harm" to the individual. Violations of the breach notification obligations can result in punishment, including fines up to $100,000.

As mandatory notification is adopted by more jurisdictions, it will increase the potential for lawsuits, as more individuals are made aware of potential breaches of their privacy that may otherwise have gone unpublished. It also has the potential to increase costs for companies in the event of large-scale breaches, in which thousands or potentially millions of customer records are compromised. Under a mandatory-reporting regime, companies are required to notify all affected individuals of the breach – an expensive proposition, particularly in the absence of insurance coverage.

Coverage Issues

In the past, many companies may have relied on their Commercial General Liability (CGL) policies to protect them in the event of a breach of privacy claim. In Canada, the standard CGL policy includes coverage under "Coverage B" for compensatory damages arising out of "personal and advertising injury," which includes "oral or written publication, in any manner, of material that violates a person's right of privacy."

Under a mandatory-reporting regime, companies are required to notify all affected individuals of the breach – an expensive proposition.

While there are few cases that consider the scope of insurance coverage in privacy breach cases, there are a number of reasons to believe a CGL policy may not offer coverage in the event of a privacy breach.

First, the tort of breach of privacy (both at common law and in statute) does not require proof of damages. Accordingly, there may be no coverage for a tort claim for breach of privacy under a CGL policy, on the basis that no actual "compensatory damages" have been incurred.

Second, breach-of-privacy claims may be framed as breach-of-contract claims or as claims for waiver of tort. As neither claim is framed in "injury", but rather, based on principles of contract and equity, a standard CGL likely would not provide coverage to a claim brought on these causes of action.

Third, even if no lawsuit is commenced, the cost of notifying all affected individuals of a privacy breach can be significant. Under a mandatory-reporting regime (such as that coming into force federally in Canada), notification would likely require legal assistance to ensure that the notification meets the requirements provided for by the law. Such costs would not be covered by a CGL policy.

Finally, American case law suggests that the coverage afforded under a CGL for "publication" that violates a person's right of privacy does not include publication by a third party, such as a publication resulting from a hack or theft. In *Zurich American Insurance Co. v. Sony Corporation of America*,[18] a case arising out of the 2011 hack of Sony PlayStation Network, the New York State Supreme Court held that "publication" required the publication to be made by or on behalf of the insured, and not unauthorized publication by hackers. As the privacy breach resulted from the unauthorized criminal activities of third parties, the court found the insurers had no duty to defend Sony against the underlying lawsuits seeking damages arising out of the publication that violated user privacy. This decision was appealed, and the appeal was settled before the appellate court ruled on the issue.[19]

The increase in lawsuits and potential coverage issues associated with the standard CGL has led many insurers in Canada to offer specialized cyber-liability insurance, which can include coverage for lawsuits arising out of privacy breaches, as well as the costs associated with forensic investigation of the breach, notification of affected individuals, and regulatory penalties for failing to comply with privacy legislation.

To date, there are no cases in which such policies have been interpreted by the courts. However, given the potentially astronomical costs in the event of a breach, companies should ensure they have evaluated their potential exposure to claims arising out of privacy breaches and taken the necessary steps, including arranging appropriate insurance coverage, to ensure their business can recover from a privacy breach.

Daniel Reid is an associate with Harper Grey LLP, practising in the areas of defamation and privacy. 604.895.2877, dreid@harpergrey.com

Licensees can earn a CE technical credit. Go to *www.thelearningportal.ca/ibabc*

[18] *Zurich American Insurance Company v. Sony Corporation of America*, et al., Index Number: 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).

[19] http://law.justia.com/cases/new-york/appellate-division-first-department/2015/651982-11-14547-14546.html

Index of Advertisers

Allianz Global 21
www.allianz-assistance.ca
Aviva 23
www.avivacanada.com
B&W Insurance 39
www.bwinsurance.com
BC Broker Digital 37
www.ibabc.org
BC Insurance Directory 33
www.insurancewest.ca
Carfra Lawton 15
www.carlaw.ca
CNS 40
www.cns.ca
Coast Claims 38
www.coastclaims.com
HyperArticles 25
www.ibabc.org
IBABC Education 17
www.ibabc.org
ICBC 2
www.icbc.com
Intact Insurance 4
www.intactinsurance.com
Metrix 19
www.metrixprofessional.com
Pal Insurance 13
www.palcanada.com
Reliance Glass 27
www.relianceglass.ca
Sovereign General 29
www.sovereigngeneral.com
Vickerstaff Dinner 35
www.ibabc.org
Winmar Restoration 9
www.winmar.ca