Stikeman Elliott

REPRESENTATION AND WARRANTY INSURANCE IN TECHNOLOGY M&A

INCREASINGLY COMMON IN M&A GENERALLY, RWI RAISES SPECIAL ISSUES IN TECHNOLOGY CONTEXTS, WRITES **ALETHEA AU** OF STIKEMAN ELLIOTT

REPRESENTATION AND WARRANTY INSURANCE (RWI) has become an important tool for transactional risk management. When an M&A transaction involves a technology business, insurers underwriting RWI tend to focus on a few key areas of risk, including cybersecurity, privacy, tax, and cross-border issues. By focusing their diligence in the same areas, acquirors – who are typically the insured in RWI policies – may be able to:

- minimize or avoid exclusions and limitations in RWI coverage that might otherwise be imposed by the insurer; and
- achieve appropriate risk allocations where such risks do necessitate exclusions and limitations in RWI coverage.

This article examines these key risks and how they may affect RWI coverage and acquiror due diligence in technology-focused M&A transactions.

1 Cybersecurity and privacy

It is no surprise that cybersecurity and privacy top the list, particularly when the target business collects, stores, handles, and otherwise processes personal or other confidential information, or where it is a provider of IaaS or SaaS (or has a material reliance on such a provider).

Factors on which insurers typically focus include:

- cybersecurity protections against cyber attacks;
- the nature of the target's business (e.g., B2B or B2C);
- jurisdictions and regulatory environments in which the target operates;
- types of data involved (e.g., personal, financial, or sensitive information);
- business continuity and disaster recovery plans (availability and how tested);
- target's data breach history, if any (and responses to such incidents);
- any material privacy or regulatory complaints, investigations, or orders; and
- underlying insurance coverage (e.g., cyber and E&O).

Insurers expect target companies to have obtained cybersecurity insurance coverage that is appropriate, in amount and scope, for their type of business. When it comes to breaches of privacy and cybersecurity-related representations, RWI coverage is typically provided only on terms that are no broader than those of the existing cybersecurity policy and only on losses in excess of that existing coverage. In other words, if the scope of the target's cybersecurity insurance is inadequate for a business of its type, the consequence could be that the purchaser will be left with an RWI policy that covers losses only above a threshold amount or that offers only a limited scope and/or coverage amount for cybersecurity matters.

2 Taxation-related risks

Technology businesses are often subject to heightened tax risks that can affect potential acquirors and insurers.

Misclassification of employees

The technology sector's reliance on contract workers can create a "misclassification" risk: if the work arrangements of the target's "contractors" bring some or all of them under the legal definition of "employees," the target may face significant liabilities with respect to uncollected withholdings and payroll taxes.

Applicability of sales tax

Depending on the nature of the product or service provided and its fee structure (e.g., subscription fees for a service, royalties, licence fees, etc.), sales tax may be applicable in some or all Canadian jurisdictions. Targets may in some cases have failed to collect and remit such taxes when required.

If the target is a digital goods and services supplier that supplies Canadian customers directly, Canadian law requires that it register to collect value-added tax (GST/HST) from such customers, even if it has no physical presence in Canada (customers that are themselves registered under the GST/HST collection regime are excluded). Failure to collect and remit such taxes could create a tax liability for a target.

Investment Tax Credits (ITCs)

For Canadian technology companies, applicable federal and provincial Scientific Research & Experimental Development (SR&ED) tax incentive programs may provide investment tax credits to claimants. Qualifying target companies may receive benefits in the form of a refundable investment tax credit (i.e., a cash payment even if there is no tax to reduce), a reduction in taxes payable, or both.

Because ITCs translate to real dollars, they may have an impact on the valuation of the target. Where that impact is material and could materially affect the quantum of losses claimed, insurers tend to review closely a purchaser's diligence efforts to verify and validate the target's ITCs.

3 Risks arising from the multijurisdictional nature of technology businesses

While today's technology businesses are built to transcend borders, the laws that

govern them are tied to individual jurisdictions. Insurers are attentive to a number of cross-border legal risks, including those discussed below.

Multijurisdictional workforces and customer bases

Technology company workforces tend to be mobile. For example, development teams may be physically located in another jurisdiction or even spread across multiple jurisdictions. Customers of such companies also tend to be located in many jurisdictions. As a result, even relatively small targets in the technology area may raise significant cross-border issues that will attract the attention of insurers.

Technology transfer – cryptology and other sensitive areas

Where a technology target's offerings involve cryptology and/or have been transferred outside the target's home jurisdiction, insurers will focus on the added compliance risks in the trade law/sanctions areas discussed below.

Economic sanctions

Involvements with foreign entities and nationals, whether as customers or as investors, can sometimes be problematic. At the start-up stage, a technology company may be focused on finding investors and customers without a great deal of regard to their locations or backgrounds. As the exit stage approaches, however, purchaser diligence may include investigating compliance with economic sanctions laws, including (in Canada) relevant provisions of the Special Economic Measures Act, United Nations Act, Freezing Assets of Corrupt Foreign Officials Act, the Sergei Magnitsky Law and the Criminal Code, to ensure that the target has no involvement with sanctioned entities.

As is the case with violations of export compliance laws in respect of cryptology, it is difficult in a typical transaction timeline to accurately quantify the damages that may arise in addition to potential imposition of fines for violating the laws listed above. Internal investigation and reporting costs can be very high. As a result, insurers are often unwilling to assume these risks.

RECENT OBSERVATIONS

High-deal volumes in 2021, increased RWI claims activity (based on accumulation of historical claim data), and insurers' capacity constraints have led to, among other things:

- an increase in premiums (especially where enterprise values are below $10 million);
- increased reluctance by insurers to provide quotes or the provision of quotes that signal additional exclusions;
- more tailored COVID-19 exclusions; and
- increased focus on diligence.

As a result of the higher cost of RWI in H2 of 2021, we have observed a growing tendency for buyers to self-insure. This trend is particularly strong among strategic buyers that are knowledgeable in the target's industry and practices. This and an easing of capacity constraints for insurers could lead to a more stable equilibrium in the market for RWI in 2022

Alethea Au
Partner, Toronto
Stikeman Elliott
+1 416 869 5514, aau@stikeman.com