**DATA COLLECTION AND DATA SECURITY: AN INCREASINGLY IMPORTANT CONCERN FOR M&A TRANSACTIONS**

The most recent market trends indicate a significant increase of the role of privacy matters within M&A transactions, with a particular focus on potential data security issues. In this scenario, the parties involved in M&A transactions have opposing interests, both aimed at managing their respective transactional risks and related consequences.

The seller, on the one side, is expected to give representations and warranties in respect of the target business and, therefore, is required to take into appropriate consideration the increasingly significant field of data security. The buyer, on the other side, must ensure that it conducts appropriate privacy and data security due diligence on the sellers and/or target companies and that the purchase or merger agreement's provisions (in particular, the R&Ws given by the sellers) adequately address the target business and its past and current practices.

**1. Data breach: an underestimated (and partially unknown) phenomenon**

Verizon has recently published its "*2016 Data Breach Investigations Report*" regarding (i) data breaches (incidents that result in the confirmed disclosure and not just potential exposure of data to unauthorized parties) and (ii) information security incidents (security events compromising integrity, confidentiality or availability of information assets) affecting organizations in 82 countries and across a very large number of industries, demonstrating that "*no locale, industry or organization is bulletproof when it comes to the compromise of data*".

Some numbers: The 2016 dataset was made up of over 100,000 incidents, of which 3,141 were confirmed data breaches and, of these, 64,199 incidents and 2,260 breaches comprised the finalized dataset that was used in the analysis and figures throughout Verizon Report. Although it seems a very complex framework, over 90% of the numerous incidents and breaches fell into one of "*the nine incident classification patterns*" created by Verizon in 2014 on the basis of the recurring combinations of "who" (actors), "what" (assets), "how" (actions) and "why" (motive), among other incident characteristics (wording taken directly from the Report):

(i) Web App Attacks: any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms;

(ii) Point-of-Sale Intrusions: remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets;

(iii) Insider and Privilege Misuse: all incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well;

(iv) Miscellaneous Errors: incidents where unintentional actions directly compromised a security attribute of an information asset;

(v) Physical Theft and Loss: any incident where an information asset went missing, whether through misplacement or malice;

(vi) Crimeware: any incident involving malware that did not fit into a more specific pattern. The majority of the incidents that comprise this pattern are opportunistic in nature and have a financial motivation behind them. This pattern frequently affects consumers and is where "typical" malware infections will land;

(vii) Payment Card Skimmers: all incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card (*e.g.*, ATMs, gas pumps, POS terminals, *etc*);

(viii) Cyber-espionage: incidents which include unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage;

Denial-of-Service Attacks: any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

**2. Yahoo – Verizon deal: a true story**

In addition to the above data and numbers included in its latest annual Data Breach Investigations Report, Verizon directly experienced the increasing importance of addressing the risk of a data breach when negotiating an acquisition.

As many media outlets reported in December 2016, the $4.8 billion acquisition between Yahoo Inc. and Verizon Communications Inc. (announced in July) is actually on stand-by due to the confirmation made in September by Yahoo regarding two different data breaches (one in 2013 and one in 2014) affecting more than one and half billion of its user and customers e-mail accounts (which involved also some large law firm in the US). For the time being, Verizon has at least three options currently under evaluation: (i) stepping away from the deal, probably by triggering a material adverse effect clause; (ii) negotiating a lower price for the acquisition; or (iii) having Yahoo assume responsibility for lasting damage caused by the breaches.

Regardless of the decision Verizon is going to make, this case clearly shows that the risk of data breaches is taking on a bigger role in M&A agreements and, therefore, more specific representations about data security, compliance with privacy laws, data breaches and hacks should now be included in SPAs and other transaction documents.

But this scenario does not only refer to an agreements' drafting and negotiation stage: preliminary surveys and analysis made by the potential buyers should be more focused on these "new" areas of risk, whether by means of specific requests within the due diligence process, or by investigating the incident history of the target company regarding previous data breaches and relevant remedies, or through deeper examinations of the relevant regulatory compliance.

Given the above, buyers could also require from the seller's management some kind of assessment, which could trigger their liability in case of untrue or reticent representations, without prejudice to additional specific statements made by the seller to address the risk of a breach. This will, of course, be included within transaction documents, requiring strenuous negotiations for providing limitations or qualifications such as knowledge qualifiers or time limitations.

**3. How to deal with data breaches within M&A transactions: minimal hints and samples**

In light of the above, below are some very basic indications on how to handle data breach issues in M&A transactions:

a) Due diligence checklist: sample request

When assisting a buyer in a potential M&A transaction, it is advisable to make one additional request

within the Intellectual Property and Information Technology Section of the Legal Due Diligence Checklist:
"*Please provide details of any actual or potential data and information security breaches, unauthorized use or access of the Company's IT systems or data, or data and information security issues affecting the Company [in the past [*number*] years]*".
Depending on the business and the industry of the target this request may be expanded significantly.

b) Representations and warranties: sample cause

When negotiating the transaction documents, the data breach issue is usually contained in the R&Ws, irrespective of the business of the target company. Please find below a very basic sample:

"***Security Breaches and Unauthorized Use***. *[To the knowledge of the Seller,] [T/t]he Company has not[, in the past [*number*] years,] experienced any loss, damage, or unauthorized access, disclosure, use, or breach of security of any personal information in the Company's possession, custody, or control, or otherwise held or processed on its behalf*".

Whether you are on buyer's or seller's side, negotiations can lead to a well-balanced and fair wording or, alternatively, to a clause which is more favorable to one of the parties. In this respect, a limitation to the "knowledge" or "best knowledge" of the seller can be a fair concession to the seller, as well as a limitation in terms of times which, of course, will be more favorable to the seller the more the time frame is limited, and *vice-versa*.

---

**ARE YOU A CO-EMPLOYER?**

"Co-employment" may be defined as a situation characterized by two or more companies (e.g. the holding company and one or more subsidiary) having legal rights and duties over the same employee. Co-employment may represent a way to define the employment relationship among companies **organized under the same group**. This conclusion is supported by Italian case law and by the great majority of commentators.

**Two conditions** must be met in order to consider multiple companies as co-employers of an employee:

1. the working performance must be supervised by two or more companies of the group; and

2. the same performance must be aimed at reaching a group interest.

The existence of a relationship among the companies, or the fact that two or more companies are organized under the same group is not, **in itself, sufficient** to determine the existence of a co-employment relationship between the companies and the employee.

**1. Supervision exercised by two or more companies of the group**

It can be difficult to evaluate whether two or more companies of the same group are both supervising the working performance of an employee. Indeed, the holding company may exercise its control over a subsidiary without having any relationship with the latter's employee. Therefore, it may seem that the holding company has no particular role in the employment relationship.

According to Italian case law, if the holding company exercises **direction and control** over the subsidiary, then such activity may have an impact on the management of the employment relationship. However, **this may not be sufficient** to determinate whether the employee of the subsidiary company has an employment relationship with the holding company that exercises the direction and control.

The holding company may need to achieve specific production and business goals and, therefore, it may direct the activities of a specific subsidiary (or a specific department) in order to reach such goals.

Furthermore, the holding company may require compliance with particular processing techniques, technical standards, or quality standard of the final product. In such cases, the holding company exerts a dominant influence over the management and organization of the work of the subsidiary's employee. It follows that the role of the holding company is not different from that of an employer. This may lead to co-employment of the employee by the holding company and its subsidiary**.**

**2. The group interest**

**The** group interest is different from the interests of the holding company and of the subsidiaries, which are directed and controlled by the holding company.

The group interest is aimed at developing a single strategy to direct the activities of all companies belonging to the group. If the holding exercises **direct control** over an employee, then such an individual may be recognized as an employee of the holding, rather than of the subsidiary, as the latter is the one profiting from the work done by the employee. This activity carried out by the holding is illicit under Italian law ("*interposizione illecita di manodopoera*").

Conversely, if two or more companies act in order to reach a group benefit, then they may be considered as co-employers.

**3. Risks and recommendations**

Co-employment poses particular risks if an employee files a legal complaint. If successful, both the employer and the co-employer may be held responsible for any related damages. Indeed, each company would be liable for the decisions taken by the other.

To avoid such risks, the holding company shall not supervise, as far as possible, the working performances of any of its subsidiaries' employees; and such performance shall not be carried out in order to reach a group benefit, but in order to reach the interest of the employer (e.g. the interest of the subsidiary).

## SHORT NEWS

**BUSINESS JUDGEMENT RULE: HOW DOES IT WORK IN ITALY?**

The Italian Supreme Court, by means of decision no. 17761/2016, confirmed that a **director of a company cannot be considered liable** towards the company for having made **business choices that**, under an economical perspective, **have not been deemed appropriate**, since such evaluation is related to the entrepreneurial discretion. Therefore, such specific choice cannot lead to a revocation for cause of such director and the same choice cannot trigger the directors' liability *vis-à-vis* the company.

The judgement over the degree of diligence used by the director in the accomplishment of his/her mandate, may not concern management choices, methods and circumstances, even if such choices may expose the company to significant risks.

Indeed, **the judgement may only concern the diligence and care used by the director in analyzing – *ex-ante* - the risks** related to the business transaction to be carried out in the name and on behalf of the company. Therefore, exclusively **the lack of the required accuracy**, evaluations and information that are normally required for similar choices made in the same circumstances and in the same manner **may lead to the directors' liability**.

For more information on such decision, please refer to the following link.

---

**DIRECTORS LIABILITY – WHAT'S NEW FOR NON-EXECUTIVE DIRECTORS?**

**The Italian Supreme Court** (decision no. 17441/2016) **stated that non-executive directors may not be deemed liable *vis-à-vis* the Company for the actions taken by executive directors**, as a mere consequence of the breach of a general duty of supervision. Such statement is in-line with the Court's precedents issued after the Italian company law reform of year 2003.

Before such reform, the law provided that each board member (including non-executive members) was subject to a general duty of supervision over the actions of the other directors. As a consequence**,** non-executive members, could have been deemed liable for simply not having surveilled over the conducts of executives, if such conducts damaged the company.

Since the law has changed in year 2003 and there is no longer reference to such general duty of supervision, Italian judges issued several decisions stating that (i) non-executive members may not be deemed liable for actions taken by executive directors, as a mere consequence of the breach of a general duty of supervision and (ii) to be deemed liable for actions of executives, non-executive members must:

1) be aware that such actions may damage the company and not take any action to prevent the potential damage;

2) not gather further information and ask executives for explanations in case a certain transaction appears to be dangerous for the company.

The decision of the Supreme Court at hand is in line with the above described principles.

Furthermore under a different perspective, the same decision stated that the **directors' liability for damages caused to the company** shall be deemed as a contractual liability.

Therefore, the company has the burden to:

(i) indicate the specific violations committed by the director in breach of his duties;

(ii) prove the damage suffered;

(iii) prove that such damage directly arises from such specific violations.

In order to defend his/her behavior, **the director must prove** that he/she acted in compliance with the duties provided by the Italian civil code. In particular, the directors granted with managing powers may be held liable if they do not observe the professional duty of care.

This general rule applies **without prejudice to the application of the business judgement rule**, under which the business decisions made by the directors may not be subject to the Court's judgement, unless such decisions – if evaluated *ex-ante* – have been **clearly imprudent and rash**.

For more information on such decision, please refer to the following link.

---

The previous newsletter numbers are available on our website.

If you want to subscribe click here.

Follow us: