HOW WILL FRANCHISORS IN EUROPE MEET THE CHALLENGES OF THE PROPOSED CYBERCRIME DIRECTIVE?

Dr Mark Abell, Graeme Payne *and* **Joseph Jackson**, *Bird & Bird, London, UK*

Cybersecurity is arguably receiving more attention than ever. For businesses that benefit from the opportunities afforded by today's digital marketplace, the past decade has seen cybersecurity move from being '*something for the IT guys to deal with*' to one of the biggest challenges to their success. The scale of the challenge is such that policymakers in Europe are considering introducing regulation on cybersecurity which, if adopted, could impact the way we do business today. This article sets out the new measures that are being considered and how many franchisors might be affected. It also suggests some of the ways that franchisors might consider meeting this challenge.

Cybercrime – a growing threat

But why regulate on this now? The catalyst for cybersecurity legislation appears to be the growing threat to business from 'cybercrime' – the use of computer technology to commit illegal offences, usually with the aim of obtaining a pecuniary advantage.

For franchise systems that fall victim to cybercrime, the consequences can be wide-ranging. Theft from online bank accounts, appropriation of trade secrets and proprietary information, business interruption, the time and expense required to investigate incidents, regulatory fines and reputational damage are just some examples of the typical fallout from a cyber-attack. Although there are no franchise specific statistics for cybercrime available, more general recent attempts at quantifying its financial impact make for concerning reading:

- A report[1] from IT security provider McAfee estimated the annual cost of cybercrime to the global economy to be $300 billion.
- In the UK, a 2011 report[2] from the Cabinet Office reported that cybercrime costs the country £27 billion each year.
- A British Retail Consortium report[3] placed the cost of cybercrime to the retail sector in the UK in 2011-2012 at £205.4 million.

[1] '*The Economic Impact of Cybercrime and Cyber Espionage*' – McAfee and the Center for Strategic and International Studies, July 2013

[2] '*The Cost of Cyber Crime*' – UK Cabinet Office and Detica, February 2011

– A 2013 report[4] from the Department for Business, Innovation and Skills found that the cost of the single worst security breach in the past year was on average £450,000 – £850,000 for large organisations and £35,000 - £65,000 for small businesses.

However, franchisors are not always the victims of cybercrime. There are some instances of them being the, possibly unwitting, instigators of or participants in it. For example, in the US there have been allegations of franchisors supporting and even directing their franchisees to become involved in cybercrime by illegally spying upon and obtaining the personal financial information of customers. On October 22, 2013, the Federal Trade Commission announced a proposed settlement with Aaron's, Inc. ("Aaron's") stemming from allegations that the franchisor knowingly assisted its franchisees in spying on consumers. Specifically, the FTC alleged that Aaron's facilitated its franchisees' installation and use of software on computers rented to consumers that surreptitiously tracked consumers' locations, took photographs of consumers in their homes, and recorded consumers' keystrokes in order to capture login credentials for email, financial and social media accounts. This is not an isolated incident as the FTC has previously settled similar allegations against Aaron's and several other companies.

The European Commission ("the Commission") views the growing threat of cybercrime as a significant barrier to completing a 'Digital Single Market' in Europe. In its strategy on cybersecurity published earlier this year, the Commission expressed its concern that consumer confidence in the online marketplace is being undermined by cybercrime. Furthermore, it found that any initiative aimed at improving Europe's cyber resilience would require action from both government and the private sector. In attempting to address these concerns, the Commission has proposed a draft Directive on cybersecurity which at the time of writing is being consulted on by Member States.

The Commission's proposed legislation – the Cybersecurity Directive

The draft Directive does not specifically refer to franchising but its overarching principle, which is to ensure a '*high common level of network and information security*' amongst Member States, has a potential impact upon it. The Commission hopes to achieve this aim by: setting governance requirements at a national level; imposing minimum cyber requirements at an industry level; and establishing a framework for information sharing on cybersecurity. These are the challenges that franchisors operating in the EU will have to meet.

"In its strategy on cybersecurity published earlier this year, the Commission expressed its concern that consumer confidence in the online marketplace is being undermined by cybercrime."

[3] '*Counting the cost of e-crime*' – British Retail Consortium, August 2012

[4] '*2013 Information Security Breaches Survey*' – Department for Business, Innovation and Skills and PwC, April 2013

"The area of the draft Directive that is likely to provoke the most interest and debate amongst franchisors concerns the minimum requirements and reporting obligations that will be placed on them."

National strategy

At a national level, the draft Directive envisages each Member State establishing a governance framework for monitoring and handling cybersecurity incidents, to include the following:

1. *A national strategy and cooperation plan on network and information security*. At the time of writing, fourteen of the twenty-eight Member States already have a national strategy on cybersecurity in place, though if the draft Directive is approved, they may be required to update their existing strategies to reflect the minimum requirements set out in the Directive.
2. *A national competent authority ("NCA") tasked with monitoring the application of the Directive*. In recognising the risk that the Directive could be interpreted differently when being implemented by Member States, the Commission proposes that NCAs shall contribute to its consistent application across the EU, though it is unclear what this would require Member States to do in practice.
3. *A Computer Emergency Response Team ("CERT")*. The role of CERTs appears to be more 'hands-on' than that of the NCAs and includes monitoring and responding to cybersecurity incidents, raising public awareness of cyber risks and forging cooperative relationships with the private sector.

Franchisors should be aware of the implementation of these measures and be alive to the impact that the national framework could have on their operations and franchisee network.

Industry-level requirements

The area of the draft Directive that is likely to provoke the most interest and debate amongst franchisors concerns the minimum requirements and reporting obligations that will be placed on them. If adopted, the draft Directive would require certain franchisors to '*take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations*'. Furthermore, such franchisors would be obliged to ensure that their systems '*guarantee a level of security appropriate to the risk presented*', having regard to the current state of the art. That could be a heavy burden for franchisors.

Perhaps more significantly, franchisors with systems falling within the draft Directive's scope would be required to report to their NCA any incident within the system that has a '*significant impact on the security of the core services*' the franchise systems provide. The implications for the Franchisor's policing of its system is clear and could be rather arduous. NCA's would then be permitted to disclose any reported incident where it determines that it would be in the public interest to do so. Franchisors subject to the Directive's reporting requirements may well fear the potential repercussions and reputational damage that could flow from public disclosure of their cybersecurity breaches.

"Franchisors subject to the Directive's reporting requirements may well fear the potential repercussions and reputational damage that could flow from public disclosure of their cybersecurity breaches."

Which franchisors will be affected?

This will depend upon the type of business the franchisor has and what sort of suppliers it works with. The fact that a business is a franchise is "*per se*" irrelevant. Broadly, the Commission appears to have three types of organisation in the cross-hairs of its industry-level obligations:

1. *Providers of information society services which enable the provision of other information society services.*

   The Directive sets out a non-exhaustive list of such undertakings which includes e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services and application stores. In practice, a broad interpretation of this group would cover businesses with an online sales presence. Franchisors who provide technology infrastructure for their franchise network would most likely be caught.

2. *Operators of critical infrastructure essential for the maintenance of vital economic and societal activities relating to energy, transport, banking, stock exchanges and health.*

   Any franchisors operating in these sectors are potentially at risk of coming within the provisions of the directive.

3. *So-called 'public administrators'.*

   The draft Directive does not define this group, though it is widely assumed to cover public sector bodies, and so is less likely to be of immediate relevance to franchisors, unless their client base or suppliers are such public sector bodies. Franchisors which provide services to the public sector, such as home care for the elderly, may find that the commercial reality is that the regulatory burdens are passed on to them by their public sector clients.

An exemption will apply to franchisors (and other businesses) that are deemed to be a '*microenterprise*', or in other words, franchisors with fewer than ten employees and with an annual turnover of €2 million or less. However, the key point for franchisors here is that it is not yet clear how this exemption would be applied to a franchising model and whether franchisees would be deemed part of the franchisors' business. If they are not, many mid-sized and small franchisors and their franchisees may be able to squeeze themselves out of the Directives point of impact. However, if the franchisor and its franchisees are aggregated most franchises will come within the ambit of the Directive. Similarly, it is uncertain whether franchisees will be aggregated together for the purposes of the exemption.

It should be remembered that, as part of the '*technical and organisational measures*' that undertakings would need to adopt, businesses caught by the scope of the draft Directive may seek to impose cybersecurity obligations on their supply chain through their commercial contracts. The scope of businesses impacted by the Commission's industry-level requirements may therefore extend beyond those referred to in the draft Directive.

"... businesses caught by the scope of the draft Directive may seek to impose cybersecurity obligations on their supply chain through their commercial contracts."

"Whatever the final form of the Directive, it is likely that changes to franchisors' current agreements will be necessary and franchisors will have to ensure compliance by their franchisees throughout the EU."

What happens if a franchisor does not comply?

The draft Directive requires Member States to set their own '*effective, proportionate and dissuasive sanctions*' for failure to comply with the industry-level obligations set out above. It remains to be seen what form such sanctions will take.

The Commission has proposed that NCA's will be given wide powers to investigate cases of non-compliance with the Directive, which some may fear to be too intrusive. Franchisors who operate a network to which the draft Directive applies will be required to provide their NCA with all information required to assess the security of their networks, including documented security policies. Furthermore, NCAs could compel audits of such franchises and issue other binding instructions. A franchisor with a presence in a number of EU member states could therefore have to contend with a number of different NCA's all taking a slightly different approach to enforcement of the Directive.

Information sharing

One of the centrepiece proposals of the draft Directive is to establish a 'cooperation network' comprising the Commission and the NCAs of each Member State to facilitate communication on cybersecurity issues. The draft Directive envisages the cooperation network being used to circulate early warnings on risks and incidents, exchange best practices on cybersecurity and conduct peer reviews of the cyber capabilities and preparedness of Member States.

With regards to early warnings, the NCA for each Member State would be obliged to report to the cooperation network any risk or incident that could either grow rapidly in scale, exceed national capacity or affect multiple Member States. Where such incidents are reported, the draft Directive requires NCAs to agree on a coordinated response. This aim perhaps seems rather ambitious and one has to question whether 28 Member States will be able to swiftly agree on a response to cyber incidents in practice. This clearly poses some challenges to franchisors which operate in several EU countries.

The future – challenges for businesses

The draft Directive is still very much in its early stages and so it is not possible to give a detailed analysis of its potential impact upon franchisors and their networks or the steps that they will be required to take to protect their best interests and those of their franchisees and customers. This presents franchisors and their trade associations the opportunity to try and influence the deliberations of the Commission and so shape the final form of the Directive to ensure that it does not impose unduly heavy burdens upon franchisors and their systems in the EU.

Whatever the final form of the Directive, it is likely that changes to franchisors' current agreements will be necessary and franchisors will have to ensure compliance by their franchisees throughout the EU.

The draft Directive also leads one to wonder if and when other countries will address the cybercrime issue, and if so, how. Some like Singapore have already done so in a somewhat different manner to that proposed for the EU. A heterogeneous approach to cybercrime across the world is going to make life potentially very interesting for international franchisors, in much the same way as the differing approach to privacy and data protection taken by the US on one hand and the EU on the other, has done.

Dr Mark Abell, Graeme Payne and Joseph Jackson

Mark Abell is a partner in the international law firm Bird & Bird where he is global Head of the Franchising, Licensing and Multi-channel Strategies team. He advises a wide range of household names on the international expansion and the re-engineering of their businesses. Having written his doctoral thesis was on "The Law and Regulation of Franchising in the EU", Mark is the author of 9 books on franchising and licensing and has acted as an expert to the WIPO and WTO on franchising and is co-editor of the International Journal of Franchising Law. He is also a member of the IBA Franchise Committee, and the ABA Franchise section (mark.abell@twobirds.com)

Graeme Payne is a partner in the Franchising Licensing and Multi-Channel Strategies team at Bird & Bird LLP. He advises a number of house hold names in the retail, leisure, food & beverage, services and healthcare sectors. He has particular expertise in advising businesses on the use of franchising as a tool for strategic growth and expansion. He is the author of chapters on franchising in several books and is a regular speaker around the world on franchising issues. (graeme.payne@twobirds.com)

Joseph Jackson is an associate in the commercial practice at Bird & Bird LLP. His practice covers a broad range of commercial matters, though he has a particular focus on IT, technology and digital media. Joe regularly engages with industry on cybersecurity issues and recently assisted the British Standards Institution on the drafting of its publically available specification on cybersecurity. (joseph.jackson@twobirds.com)