Getting the most from customer data – a key asset for franchising growth

December 2013

Getting the most from customer data – a key asset for franchising growth

Introduction

Increasingly in the future, when an international franchising business is asked to identify its most valuable asset, it may well point to its customer data. Inexhaustible developments in technology and the rise of technology for the masses mean that businesses now have access to information about how their customers tick as never before. Whereas a business might previously have run a marketing campaign based on focus group feedback, now it can target its marketing based on how individuals visit its website and use its app (on tablets as well as smartphones), as well as how they rate and recommend it on social media. Moreover, a business can perform this analysis of customer interactions on staggering amounts of data.

Opportunity

The world markets have opened up and franchisors have looked to internationalise by exploring new territories, frequently in the Far East. The opening up of certain 'goldmine' territories (eg, China) to franchisors offers the promise of substantial growth. In many of these territories, major franchisors' brands are already widely known and an engaged customer base already exists. In other territories and for many brands, it will take more time to build up a loyal customer base, and franchisors may look to social media and their online presence to generate interest and gauge reaction.

In the offline world, franchisors will increasingly want to provide the same in-store experience to a loyal customer, whether that customer is in a franchisee store in Manchester or Moscow. Franchisors that deliver a seamless service in which customers feel special and customer needs are anticipated based on astute data marketing and analysis can reap a massive loyalty reward. Effective use of customer data can exploit the personalised offline experience in an online setting. It can enable franchisors to respond more quickly to customer trends and develop an integrated approach to marketing and brand-building campaigns. Franchisors that embrace this approach should ensure that teams are structured around the customer and not just the channel, thus guaranteeing more integrated collaboration between the corporate-owned business and franchise-owned business.

Data protection rules on a global stage

Any handling of customer data is likely to trigger the application of data protection and privacy rules. Issues of intrusiveness and data security concerns have increasingly led to more countries legislating for data protection. For instance, in recent months Singapore and South Africa both passed data protection laws. However, the standard that remains the strictest is that set out in the EU Data Protection Directive (95/46/EC). As those who have dealt with the Data Protection Directive before will know, there are restrictions on the transfer of personal data outside the European Union. This restriction can be perplexing for international businesses that are keen to push into new geographies such as the European Union. Nonetheless, there are ways of meeting the data transfer compliance requirements, such as through the comparatively new innovation of binding corporate rules, which a number of truly global companies have now adopted (including, for obvious reasons, a major international hotel group). What makes the binding corporate rules solution so unique is that it establishes a framework for global data protection compliance inside a multinational organisation that is consistent, even though it crosses borders, and thus builds trust – it is not concerned solely with the technical requirement to transfer personal data legitimately. Being 'joined up' and consistent is also becoming more necessary than ever before, particularly given the risk of brand damage and new legal liabilities emerging under new legislation. Customers could take fright and opt out in droves, depriving franchisors of the ability to mine and exploit these new communications channels. Getting this right will soon be seen as absolutely essential for consumer-facing brands in most sectors, and not just the obvious ones.

Gaining customers, building trust

Compliance with data protection rules – which may have been seen in the past as an obstructive, legalistic requirement – can actually be central to building trust and loyalty with individual customers. An individual who understands how his or her personal data is being used, and who has an element of choice about how it is used, is much more likely to share that data with an

organisation. On the other hand, because of greater consumer awareness and concern about the potential abuse of customer data, an organisation that is cagey about its collection and use of personal data or that gives individuals little choice may well lose customers. In a technology-driven age where more people are aware of their privacy rights, a brand that demonstrates that it 'gets' privacy will have an advantage over its competitors.

Who must comply with data protection rules?

In the European Union, the law places compliance obligations on data controllers – those organisations that make decisions about personal data collection and use. A data controller may engage service providers (known as 'data processors') to carry out some of the data processing on its behalf, but the data controller is ultimately responsible. Data controllers have quasi-ownership rights over the personal data collected, so it is crucial in any franchise relationship to establish who the data controller is and whether there is more than one. For instance, the franchisor will nearly always be the data controller of customer data, but a franchisee may be either a data controller or a data processor, depending on the arrangement between the parties. The franchisor and franchisee are usually independent data controllers – that is, they both have rights to access and use the personal data, but for their own separate purposes. A franchisee may be a data controller of customer personal data even if the franchisor lays claim to IP rights in the data. The important thing is to ensure that the parties agree on their roles and that, to the greatest extent possible, this is documented in the contract.

What does data protection compliance look like?

EU law will apply to organisations that are established (ie, operate a business, branch or subsidiary, including a franchise) in an EU member state and collect customer data. An organisation caught by EU law will need to put in place processes that meet the requirements of local law, including:

- registering with the local data protection authority;
- providing notices to individuals;
- obtaining marketing consents;
- granting access to data; and
- ensuring appropriate data retention and data security.

Certain EU jurisdictions have slightly more prescriptive rules in some areas – for instance, Spanish law sets out very specific requirements on data security. In particular, franchisees and franchisors will want to understand the rules around marketing and how they can best use technology to connect with their audiences.

Managing franchisees

A franchisor will also need to consider its strategy for managing franchisees and, in particular, what rights it has over customer data held by the franchisee. If a franchisor wants the right to control e-marketing campaigns for all customers, its franchisees are likely to be required to share access to customer databases with it as a matter of course. If this is the case, the parties will need to think carefully about what customer consents are required. Alternatively, a franchisee may want a certain amount of discretion to run local marketing campaigns suited to the specific territory (eg, a promotion for Chinese New Year).

While perhaps not an issue to dwell on at the beginning of a franchising relationship, the franchisor will also need to consider what happens to customer data where:

- one party breaches the franchising agreement so that it terminates;
- the franchising agreement expires; or
- the franchisor or franchisee is acquired by a third party.

A franchisor will usually want to ensure that a former franchisee cannot compete in the market with the new franchisee, and should thus include a mechanism in the franchise agreement to regulate the ongoing rights to use – and the obligation not to use – customer data. Competition laws should be taken into account in ensuring the effectiveness of such restrictions.

Loyalty schemes

The success of various loyalty schemes has highlighted the fact that people are prepared to give away access to

Getting the most from customer data – a key asset for franchising growth

much of their data if they receive a benefit in return. Loyalty schemes are not in themselves a new phenomenon, but new technology has given companies much greater access to information about customer behaviour and preferences. Franchisors and franchisees can take advantage of the new insights obtained through 'mining' the data captured by loyalty schemes to get to know their customers and provide them with benefits which keep them loyal. It is significant that the company behind one of the most successful UK loyalty schemes – Aimia, which runs the Nectar card programme – developed a set of data values (known as the Transparency, Added Value, Control and Trust (TACT) Rules) that places consumers at the heart of its data management activities. Good privacy practices can enhance trust and brand recognition for franchisors – and the deeper the relationship that the franchisor builds with its customers, the greater the rewards.

Multi-channel approach

Now more than even before, a franchisor can engage with customers across a variety of channels. Franchisors will be keen to ensure that, as they expand, their online presence remains consistent and on message. However, websites that target particular geographies (eg, by providing web pages in the local language or local currency) should increasingly think about compliance with local data protection requirements. For instance, the privacy notice on the website may need to be amended to comply with local law. Likewise, franchisors should consider what happens to the customer data collected through that website. Will the franchisor share it with the local franchisee so that it can target the customer? If so, does the franchisor need to obtain customer consent to do so? Of course, a franchisor can choose to give its franchisees the freedom to modify the relevant web pages to reflect the local market. There is emerging evidence that this is a particularly successful model, although franchisors will still ultimately want a significant degree of control over how the country franchisee runs the content and engages with customers. Privacy and data protection rules are still adjusting to the rapid growth of apps, but this will continue to become an extremely popular way for individuals to purchase goods in the future – take the huge success of the Domino's Pizza app, for example. Tech-savvy consumers (especially the youth market) will expect to be able to interact with their favourite brands from their smartphone or tablet. Franchisors that can spot the best ways to engage with customers through technology have the potential to gain the most.

Customer data in the cloud

It is no surprise that a number of drivers have led companies to use cloud services to store their customer data. The drive to reduce costs and the need for greater data security resilience (typically found in highly sophisticated tech companies offering cloud services) are just two factors that have encouraged businesses to move to cloud services. All franchisors (whether operating global businesses or tech-savvy domestic businesses) that involve the collection and analysis of customer data are thus likely to consider storing data in the cloud. Where the customer data is subject to EU data protection rules, franchisors should consider how to meet their obligations and reduce the risk of non-compliance. Many, if not most, of the big cloud players are based in the United States and have 'safe harbour' status, allowing EU data to be transferred to their companies in the United States, although a number also now have clouds limited to the European Union only. Franchisors engaging cloud providers should ensure that the contract provides sufficient reassurances about data security and access to the data, particularly if franchisees will be given some level of data access.

A helping hand to increase customer trust and interaction

Although there will be some sceptics due to the bad press that data protection has received in the past, good data protection compliance – when used together with other emerging technologies and customer engagement techniques such as social media and messaging technologies – can be a significant enabler for businesses by increasing customer trust and encouraging interaction. This can help franchisors and franchisees to know more about their customers and thus open up new and enhanced marketing strategies. The spread of privacy and data protection rules globally and the likely adoption of a new data protection regulation in the European Union will again emphasise the need for businesses to comply. However, compliance should be seen not as a drawback, but rather as a means of exploiting customer data in the most effective way possible. A failure to take data protection compliance seriously can result in serious fallout for companies, whether that entail a loss of reputation, compensation claims or regulator fines. A number of major companies have learned this to their cost when their non-compliance with the rules became public. It is likely to be only a question of time before a franchisor and its brand is similarly caught out.

For further information on this topic please contact Gordon Drakes, Chris Wormald, Victoria Hordern or David Naylor at Field Fisher Waterhouse LLP by telephone (+44 20 7861 4000), fax (+44 20 7488 0084) or email (gordon.drakes@ffw.com, chris.wormald@ffw.com, victoria.hordern@ffw.com or david.naylor@ffw.com). The Field Fisher Waterhouse website can be accessed at www.ffw.com

Gordon Drakes
Senior Associate
t: +44 (0)207 861 4525
e: gordon.drakes@ffw.com

Chris Wormald
Partner
t: +44 (0)207 861 4299
e: chris.wormald@ffw.com

Victoria Hordern
Director
t: +44 (0)207 861 4260
e: victoria.hordern@ffw.com

David Naylor
Partner
t: +44 (0)207 861 4150
e: david.naylor@ffw.com