LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Black Friday and Cyber Monday - 8 Legal Tips

by **Aideen Burke**

Black Friday and Cyber Monday - 8 Legal Tips

23rd November 2017 | by Aideen Burke

The day after Thanksgiving in the United States has become known as “Black Friday” and it traditionally marks the beginning of the Christmas shopping season. Think of the classic film from the 1940s, "Miracle on 34th Street", with the Thanksgiving day parade, Kris Kringle, and the Christmas sales frenzy that begins the next day.

The original intention with Cyber Monday was to offer a wide range of discounts on products bought online in order to compete with conventional shopping sales.

The distinctions between Black Friday and Cyber Monday are becoming blurred, with many online retailers offering discounts earlier and earlier.

Cyber Monday is a big deal - last year it was the biggest day in the history of e-commerce in the US with consumers spending $3.45 billion online. And the average US shopper last year spent $900 on the actual Friday, with the total spend across the US hitting $655.8 billion.

This shopping extravaganza has gone global and Irish and UK retailers have been happy to join in on the festivities, even though Thanksgiving is not an official holiday in this part of the world. This consumer sales trend is now fully ingrained in the Irish and UK retail markets and it is anticipated that it will be even more successful this year – whether the shopping is done in person or online.

It is estimated that 30% of Irish consumers believe their mobile will be their main shopping tool in the future and data from PayPal estimates that over 80% of Irish internet shoppers - an estimated 1.9 million people – make overseas purchases online each year with a considerable purchasing spike this weekend.

With these enthusiastic shoppers in mind, we have a few quick reminders in relation to consumer rights and how to manage online shopping in the workplace.

Buying online

If customers purchase online from a site that is based within the EU, they enjoy a statutory cancellation right, known as the ‘cooling-off’ right. The cooling-off right begins to run fourteen days from when the contract was formed, in the case of services, or as soon as the products have been received. In most cases, they are entitled to cancel the contract during the cooling-off period for any reason at all, including if they simply change their mind. There are some exceptions to the cooling-off right, such as sealed products, once the seal has been removed, or customised or perishable products.

Customers should receive products purchased online without undue delay and within thirty days from the purchase date, unless an alternative date is agreed with the seller. If they do not receive the products within thirty days, they may contact the seller and arrange an alternative date. If the seller fails to deliver the item by the new date, the customer can cancel the contract and get a full refund. Also, if delivery during the initial thirty day delivery period was essential, or the customer informed the seller that it was essential at the time of purchase, they can also cancel the contract and get a full refund, if the seller has refused to deliver the product.

Faulty products

If a customer discovers a product is faulty within six months of purchase, they are entitled to a repair. If this does not resolve the problem, they are entitled to a replacement or a full refund. Remedies for faulty products must be provided free of charge.

Direct marketing

Businesses generally need prior 'opt-in' consent to send direct marketing texts and emails, which applies equally to Black Friday and Cyber Monday emails and texts. But if a business obtained a customer's details in the context of the sale of a product or service in the last twelve months, then it may send marketing texts and emails provided that it complies with a number of conditions. All direct marketing texts and emails must include a free of charge facility to allow recipients to 'opt-out' of receiving future messages.

Online shopping at work

Many employers will allow employees to use the internet at work for personal purposes, including online shopping, within certain limitations. This can lead to issues for employers in relation to monitoring and restricting internet access by employees for non-business purposes. Employers should have policies on internet access, otherwise it may be difficult for employers to effectively restrict and monitor the use of business time and resources for online shopping.

Employer policies on internet access

Employers should have a clear written policy on whether internet access is provided solely for business purposes, or whether occasional personal use is permitted. If personal use is allowed, employers should set out the purposes for which internet access is permitted, and the conditions on which such access is granted. It is important for employers to state that that personal use of company systems is a privilege that can be withdrawn, and that internet access can be restricted at their discretion. Conditions for personal use of internet access can include requirements that such use does not interfere with business commitments, and should take place outside of normal working hours, such as during lunchtime.

Monitoring internet access

Employers have to comply with data protection laws in any monitoring of staff internet access. If internet access is monitored, employees should be informed in advance and should be informed of why monitoring is being carried out. Any monitoring of internet access should not unduly interfere with an employee's right to privacy. Even where internet access is restricted, employees still have a reasonable expectation of privacy in relation to their communications, which may include online shopping.

Excessive internet use

In extreme cases, employers may need to take disciplinary action in order to sanction excessive use of the internet for online shopping. In such a scenario, it is crucial that employers already have clearly stated policies in place on internet access, and that these policies provide that inappropriate or excessive personal internet access in breach of the employer's policy will amount to misconduct that may result in disciplinary action.

For more information, please contact Aideen Burke at aburke@lkshields.ie.

About the Authors

Aideen Burke
Partner

Aideen is Head of our Intellectual Property, Technology, Media and Data Privacy team.
T: +353 1 637 1574 **E:** aburke@lkshields.ie