Using E-Commerce to Survive COVID-19

April 6, 2020

As businesses have been forced to close their brick-and-mortar stores and we are all practicing safe distancing, COVID-19 has already had a significant impact on how we conduct business by causing more people to work remotely and redefine how we conduct business.

While the digital transformation was well underway before COVID-19 the transition to more vigorous and expansive e-commerce has never been more apparent. Amazon was set to hire over 100,000 new employees by April 1 and Zoom has replaced all face-to-face business meetings. Virtual interactions are the new norm.

Nearly all companies now use some form of online or mobile websites and/or social media to promote their businesses, sell goods or services, conduct business transactions, and connect and communicate with customers, clients, or other businesses.

For businesses that already enjoyed a robust e-commerce presence now is a good time to review and enhance e-commerce strategies. For those businesses with a limited or non-existent online presence the very survival of their business may require a fresh look at e-commerce.

If you do not have a website, or if it has been a few years since you last gave your site a facelift, now is the perfect time to update your website and make sure you are well positioned for e-commerce.

Here are some legal issues and practical steps a business can take to minimize risks with operating an e-commerce business.

1. Agreements with Online Service Providers. Your website may be the primary invitation for your customers to consider and purchase products and services. It can be customized to express your own unique style and needs and provide a competitive advantage. When hiring a vendor to design your website make sure you have an appropriate agreement to not only cover commercial issues such as payment and deliverables but also addresses intellectual property ownership, clearance of third-party rights, data privacy, security and confidentiality, and search engine optimization practices. If a vendor will be hosting your site and customer data make sure you consider responsibility and liability for any data breach, service levels, the return of customer data, and transition assistance upon termination. Linking and framing, clickware (and

shrinkware), and metatag use should also be considered. Agreements with service providers who process personal data on your behalf should be reviewed for compliance with the European General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

2. Customer Agreements. Traditional legal contract principles apply to transactions conducted online. This means that each online contract requires an offer, acceptance, and consideration. Make sure that any subscription agreements, terms of use, or other customer-facing agreements satisfy such basic legal principles. If users are able to post content include appropriate notices and disclaimers to limit the company's liability. What jurisdiction and governing law apply and should arbitration be mandatory?

3. Domain Name Selection. Domain names serve as your street address on the internet. In selecting your domain name be wary of any third-party trademark rights that may attach to a particular URL. Your use of a domain could violate a third party's trademark rights.

4. Intellectual Property. Safeguard unique and proprietary content that appears on your website or social media pages from unauthorized commercial exploitation with proper use of a ™, ®, and/or © symbol in connection with trademarks and copyrights. When appropriate register copyrights and trademarks with the applicable authorities. Review content and any material before display or launch to ensure that no infringing material is published and no confidential proprietary information is inadvertently disclosed on your site.

5. Update Website Privacy Policy and Terms of Use. A vast amount of customer information is collected via the website through customer registration and as part of the purchasing process. The collection, use, and sharing of any personal data is now protected and restricted by global data privacy and protection laws and regulations.

Make sure your website privacy policy and terms of use are prominently displayed, carefully drafted, and current with all relevant data privacy and security laws such as the GDPR and CCPA. The CCPA became effective January 1, 2020 and requires specific disclosures in the privacy notice and actions to comply with data access rights afforded California residents. The CCPA also allows for a private right of action with statutory damages and enables class action lawsuits against a business that experiences a data breach and failed to implement reasonable data security. Despite efforts to delay CCPA enforcement set to commence July 1, 2020, the California Attorney General has announced that it will not delay enforcement due to COVID-19.

6. Review Your Use of Social Media, Email, and Text Messaging for Marketing Purposes. Make sure administrative access and control of social media accounts such as Facebook are current. Use of email and text messaging to reach customers must comply with laws such as CAN-SPAM and Telephone Consumer Protection Act (TCPA). Failure to comply with the disclosure and consent requirements of the TCPA could

result in expensive litigation.

7. When Selling Third-Party Products Online Consider Contracts With Such Third Parties and Potential Liability. Some companies operating online marketplaces have faced multiple lawsuits for defective products such as blenders, coffee makers, and hair dryers based on claims of strict liability, negligence, and breach of warranty.

The terms of use on your website should explain your relationship with both customers and vendors and detail what rights a customer has to cancel or return purchases.

8. Managing a Data Breach. It is not a question of if you will experience a data breach but when. The CCPA private right of action in the event of a data breach is good reason to conduct a data security audit as necessary to make sure that your business is ready to handle and respond to any unauthorized access of your system and any customer data. Every business should have in place an incident response plan and information security program that describe how it handles discoveries of unauthorized access of data and what security safeguards, policies, and procedures are in place. If you experience a data breach you may have obligations to report the breach to the state attorney generals and any individual whose data is compromised. The obligation to notify will be based on the state law where the individual is a resident. All 50 states now have data breach notification statutes with varying definitions of what constitutes a notifiable data breach.

The move to remote working raises new cybersecurity issues.

9. Consider Insurance. Insurance can be a useful tool to mitigate risk related to a data breach by covering computer forensic, legal, notification, and other costs related to such breach as well as coverage to limit financial exposure for online tort and intellectual property right infringement claims, and certain website-specific practices such as hyperlinking, framing, using metatags, and banner advertising.

These are unprecedented times that require businesses to find ways to stay relevant and current. A solid e-commerce strategy may not only have an impact on the present, but give you a competitive advantage when it is safe to reopen your doors in the ever expanding digital marketplace.

For additional information, please contact Michael Cohen or your regular Lathrop GPM attorney.