Is your company transitioning from brick-and-mortar retail to online sales? If the answer is yes, pay close attention to these laws.

According to recent financial data, American shoppers are on course to surpass total online spending in 2019 by early October, as a result of the explosive growth in ecommerce inspired by the COVID-19 pandemic. Financial analysts expect continued growth in online spending due to the extension of COVID-19 lockdowns and restrictions across the country, so companies are naturally shifting more of their focus to online sales.

If your company is in the midst of a transition from brick and mortar retail to online sales or looking to expand your existing online operations as result of the COVID-19 pandemic, you will want to make sure that you are in compliance with the myriad of federal and state laws that govern the manner in which business is conducted online. In particular, your company will want to make sure that it has policies and procedures in place that ensure compliance with two of the preferred tools for regulating commerce conducted over the internet – the Restore Online Shoppers' Confidence Act ("ROSCA") and the Children's Online Privacy Protection Rule ("COPPA").

What is ROSCA and how does it affect your company?

ROSCA is a law that was enacted by Congress in 2010 to combat aggressive online sales tactics that were being utilized by certain companies. The law has two major provisions that are focused on two types of online transactions: (1) Sales by a third party to a consumer immediately following a transaction between that consumer and an initial merchant; and (2) Sales using a negative option feature.

Post-Transaction Third-Party Sales

Post-transaction third-party sellers were a major concern when ROSCA was first enacted because at the time, it was a common practice for initial merchants to transmit a consumer's payment information to a third-party, enabling the third-party to sell the consumer an additional product or service, without the express consent of the consumer. These transfers of consumer data from an initial merchant to a third-party became known as a "data pass," and it was the secrecy in which these data pass transfers were occurring (typically without the knowledge of the consumer) that caught the attention of regulators. Accordingly, ROSCA imposed the following requirements upon initial merchants and third-party sellers conducting business over the internet:

- Initial merchants cannot disclose a payment card, bank account, or other financial account number to a post-transaction third-party seller for use in any sale by a third-party seller.
- Third-party seller must make clear and conspicuous disclosures about itself and the goods or services it is offering prior to collecting the consumer's payment information; and
- Third-party seller must get the consumer's express, informed consent prior to charging him or her.

Negative Option Features

The use of negative option features in online sales

was a major concern when ROSCA was first enacted because many online consumers were enticed by the "free trial" that typically accompanied the offer and unaware that cancellation of the service after the "free trial" ended required affirmative action on their part. The definition of "negative option feature" under ROSCA is taken from the FTC's Telemarketing Sales Rule (16 C.F.R. 310), which states, "in an offer or agreement to sell or provide any goods or services, a provision under which the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer."

Common examples of negative option features are automatic-renewal subscriptions (i.e. subscriptions that involve recurring monthly payments) and continuity plans where the consumer receives a new shipment of goods on a recurring basis until they cancel the agreement (i.e. clothes, wine, food, etc.). ROSCA imposes the following requirements upon companies that utilize a negative option feature in their online sales:

- Clear and conspicuous disclosure of all material terms of the sale before collecting billing information from the consumer;
- Obtain the consumer's express informed consent before charging him or her; and
- Provide a simple mechanism for the consumer to cancel the service.

Importantly, ROSCA empowers both the FTC and state Attorneys General to enforce the law, and amidst the flood of e-commerce that is taking place during the COVID-19 pandemic, you can be certain that federal and state regulators are paying close attention to whether companies are complying with this law.

What is COPPA and how does it affect your company?

Congress enacted COPPA in 1998 to limit the collection of personally identifiable information from children under 13 without their parents' consent. When the law went into effect on April 21, 2000, the internet was not as ubiquitous as it is today, so companies that were not targeting a 13 and under audience were less concerned with whether or not they were complying with this law. However, now that children as young as five are walking around with smartphones in their pockets, playing internet-connected gaming systems, and communicating with virtual assistants like Alexa, all companies conducting business online should ensure they are in compliance with the law.

COPPA requires, among other things, that operators of commercial websites and online services directed to children under the age of 13, or general audience websites and online services that knowingly collect personal information from children under 13, must comply with the following general requirements:

- Post comprehensive privacy policies on their websites;
- Notify parents directly about their information collection practices; and
- Obtain verifiable parental consent before collecting, using, or disclosing any personal information from children under the age of 13.

It is important to note that the term "online services" broadly covers any service available over the internet, or that connects to the internet or a wide-area network. Examples of online services covered by COPPA include, but are not limited to, the following services:

- Network-connected games
- Social networking platforms or applications
- Services that allow users to purchase goods or services online
- Services that allow users to receive online advertisements
- Services that allow users to interact with other online content or services
- Mobile applications that connect to the internet
- Internet-enabled gaming platforms
- Connected toys
- Smart speakers

- Voice assistants
- Voice-over-internet protocol services
- Internet-enabled location-based services

It is important to note that COPPA includes a Safe Harbor provision that is designed to encourage increased industry self-regulation. Under the Safe Harbor provision, industry groups and others may ask the FTC to approve self-regulatory guidelines that implement the protections of COPPA. The COPPA Safe Harbor provision provides flexibility and promotes efficiency in complying with COPPA by encouraging industry members or groups to develop their own COPPA oversight programs.

A company's Safe Harbor program will likely receive FTC approval so long as it offers (1) the same or greater protections for children as those contained under COPPA, (2) effective mechanisms used to assess operators' compliance, (3) effective incentives' for operators' compliance with the guidelines, and (4) an adequate means for resolving consumer complaints. Importantly, companies that comply with their FTC-approved self-regulatory guidelines will receive safe harbor from FTC enforcement action under COPPA.

Like ROSCA, COPPA empowers both the FTC and state Attorneys General to enforce the law, and amidst the flood of e-commerce that is taking place during the COVID-19 pandemic, you can be certain that federal and state regulators are also paying close attention to whether companies are complying with this law.

Author

Shawn Collins
Shareholder
949.725.4064
scollins@sycr.com