WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Get Consumer Electronic Consents Right And Avoid Salt In The Wound

February 3, 2015

Clicking the "Accept" or "Agree" button on a website has become a daily ritual. Electronic consents have become ubiquitous because businesses of all kinds need to obtain them from customers for a host of reasons. However, many are simply doing it wrong.

Worth Getting It Right (The First Time)

A valid electronic consent from a consumer should comply with the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN Act"), as well as the Uniform Electronic Transactions Act ("UETA"), which was enacted by many states, including North Carolina. These laws have heightened protections for consumers who give consent or enter into agreements with your business electronically. Those protections include certain disclosure and procedural requirements, as well as some substantive rights. This article will not attempt to describe those technical details but, instead, is intended to persuade you that it really is worthwhile to obtain consumer consents the right way.

From time to time, business clients balk when the components of an effective electronic transaction consumer consent are explained to them. They say, "I've done business on lots of other websites, and they don't do this." There is some truth to the objection, simply because many businesses have deficient electronic consents. Most of the time, businesses that do not correctly obtain consumer electronic consents do not suffer catastrophic losses as a result. In fact, most of the time, they suffer no consequences at all. This might lead one to assume that correctly obtaining a consumer's consent is not very important. However, as my grandfather used to say, "It doesn't matter until it matters, and then it really matters." In other words, even though the probability of loss is low, the severity of harm may be high.

Getting to Yes: Is It Really Necessary?

One aspect of consumer electronic transactions that people question most often is affirmative consent. "Affirmative consent" means that the consumer expressly agrees to the terms, or "opts in." An example of an affirmative consent is the following:

> By clicking the button labeled "Accept" below, you agree to the terms and conditions of this Agreement and acknowledge that you have read and understand the disclosures provided above.

Most businesses would generally prefer negative consent, also referred to as "constructive" consent or "opt out." An example of negative consent is the following:

> Unless you notify us of your intent to opt out, you are bound by these Terms….

Obviously, negative consent is easier for businesses to obtain than affirmative consent.

However, the fact is that the UETA and the federal E-SIGN Act require businesses to give very detailed disclosures and to obtain the affirmative consent of consumers if a written disclosure or communication required by any law, regulation, or rule will be given electronically. The number of laws, rules, and regulations requiring disclosures to consumers in connection with everyday interactions is voluminous, resulting in the fact that most agreements or transactions conducted with consumers over the Internet are covered by one or more of them. (Even if you cannot think of one off the top of your head, there likely are some.) For this reason, your business should obtain affirmative consents from consumers in accordance with the law for

all online agreements or transactions.

When obtaining a consumer's consent to receive subsequent communications required by law, a business is obligated to show that a consumer has "reasonably demonstrated" that he or she can access the covered information in the relevant electronic format. Merely relying upon the consumer's assertion that he or she can receive subsequent consents electronically is insufficient. Careful businesses require evidence of the consumer's ability to receive communications in the format in which they will be delivered.

What's The Harm?

There are any number of ways in which failing to properly obtain consumer consent can have negative results for a business. The most obvious risk is that it is possible (though not certain) that a consumer consent obtained in a way that does not conform to the UETA and E-SIGN Act simply will not be effective—the consumer may be able to renege on any obligations, waivers, or the like contained in the agreement or policy. There are, however, less obvious consequences. For example, another risk that has received very little attention until now can best be explained through a hypothetical scenario: ABC Corp. sells products and services to consumers in North Carolina through its website. It has collected information from tens of thousands of consumers over the past few years, and stores that information in a database on its own server. Included in the information are the consumers' credit card numbers (so that regular customers will not have to provide all of their information every time they order) and addresses (for deliveries), among other information. The credit card numbers are not encrypted on the database. ABC Corp. becomes aware of an incident of unauthorized access to its database. Customer information likely has been accessed, and the available information indicates that the person who accessed the information has nefarious intent.

Under North Carolina law, ABC Corp. is obligated to give each consumer who is or might be affected a notice of the data security breach containing specific information. However, the North Carolina Identity Theft Protection Act provides that ABC Corp. can notify the consumers via email *only if* the consumers' consents have been properly obtained in accordance with the E-SIGN Act. While ABC Corp. has the consumers' email addresses on file, it has not properly obtained their consents to provide subsequent legally-mandated notices by email. Therefore, ABC Corp. cannot satisfy its obligations by providing the required notices by email. Instead, the Identity Theft Protection Act requires that the notice be provided in hard copy. (ABC Corp. will be required to report to federal and state agencies regarding the breach and its response, including the use of email for delivery of the required notices.) Therefore, because ABC Corp. has failed to obtain consumer consent in the proper way at the outset, the cost of responding to a subsequent data security breach, which is already likely to be tremendous, will be tens of thousands of dollars more as a result of printing and postage costs alone. At a time when ABC Corp. is deeply wounded, the additional cost is like "salt in the wound."

Better Safe Than Sorry

There are many more examples of ways in which handling a consent correctly at the start of an electronic relationship with a consumer can pay dividends later for a business. Although the benefit is not always immediately obvious, it will be prudent to consult with an expert to ensure that your business's consumer electronic consents comply with the state and federal laws and protect it from unexpected problems in the future.

--