Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

AUGUST 2016

Attorney General Reaches Six-Figure Settlement With Entity That Failed to Provide Required Data Breach Notification

A recent settlement announced by the New York Attorney General's Office has made clear that failing to provide the required notifications after experiencing a data breach can prove very costly. On August 5th, the Attorney General (AG) announced a $100,000.00 settlement that was reached after the AG discovered that an online retailer (EZcontactsUSA.com) failed to provide notice of a breach it experienced as required by General Business Law 899-aa.

Unidentified hackers infiltrated the retailer's website in August of 2014 and installed malware designed to steal the credit card information of customers placing orders through the retailer's website. That malware stole an estimated 25,000 credit card numbers and other cardholder data from the retailer's online customers between August 2014 and June 2015.

The retailer became aware of the breach in June of 2015 after its bank alerted it that fraudulent transactions were appearing on customers' credit cards. Rather than providing the required notifications, the retailer simply opted to engage a private company to locate and remove the malware from its systems. The retailer did not provide notice to affected consumers or to the various government agencies identified in General Business Law 899-aa.

The AG's investigation also concluded that, in addition to violating the notification requirements, the retailer violated additional laws by misrepresenting the security of its website. The retailer had advertised the website as 'safe and secure' and claimed that it used 'the latest security technology available' despite the fact that this was not the case. Amongst other failings, the AG found that the retailer failed to maintain a written security policy, failed to utilize effective firewall practices, and failed to deploy effective anti-virus software on their computer systems.

In addition to imposing a six-figure fine, the settlement also requires the retailer to maintain reasonable security measures going forward, remediate existing vulnerabilities, and train employees on the most up-to-date security practices.

As this settlement makes clear, it is critical for business to stay abreast of the notification requirements imposed by law, and to ensure that they comply with them in the event that they experience a data breach.

If you have any questions about this Information Memo, please contact Michael D. Billok, Clifford G. Tsan, Christopher J. Stevens or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond