Would You Like a Side of Fraud with That?

What Your Organization Should Learn from the McDonald's (and Walgreens) Breaches

12.21.2010

Kimberly A. Licata
Elizabeth H. Johnson

Last week McDonald's Corp. and Walgreen Co. notified customers that their personal information had been compromised by hackers. The hackers appear to have targeted an email provider subcontracted to a marketing firm used by both McDonald's and Walgreens. What's different about these incidents? They involved consumers' contact information, but not Social Security numbers, financial account numbers or other information that generally triggers notification obligations under breach notice laws. So why did McDonald's and Walgreens notify their consumers of these breaches? Because the stolen contact information was reportedly used to send consumers phishing emails that invited them to provide additional personal information that could be used to commit identity theft and fraud.

What Happened?

Phishing emails, which look like they are sent by a reputable company and perhaps a company with which the consumer has a relationship or account, are sent by fraudsters who hope the recipients will provide them with additional personal information that can be used to commit identity theft or access consumers' financial resources. The most typical method is to include in the email a link to a website, which also appears to be that of a reputable company, and present a seemingly legitimate request, such as verifying account information or signing up for a discount. In the course of responding, the consumer is asked to provide a Social Security number, financial account number, or login credentials to access an account, not realizing that they are providing the information to an unauthorized third party rather than a legitimate business.

Although the McDonald's and Walgreens breaches did not directly implicate the type of information that triggers state and federal breach notification requirements, the companies gave notice of the breaches. A smart move, considering both companies were arguably on notice that there was unauthorized use of contact information that could result in serious financial harm to consumers. Even without an express legal obligation to notify consumers of the breach, if either company failed to do so, relying on a technical reading of breach notice laws, and consumers became victims of identity theft or fraud, the result could have been an enforcement action alleging general unfair or deceptive trade practices by the Federal Trade Commission or state consumer protection agencies. The fact that the breach notice laws were not technically violated would have been cold comfort in that situation.

What Does It Mean for Your Company?

What should companies learn from McDonald's and Walgreens' examples? First, revisit your security incident response procedure to consider whether an incident involving only contact information would be appropriately vetted and addressed under your procedure. If not, it's a gap worth addressing in light of increases in phishing attacks and

spam. Second, revisit your service provider arrangement. By now, you hopefully have provided enhanced protections in contracts with vendors that handle Social Security numbers, financial account numbers, and the like. At this point, it makes sense to consider providing those same protections in contracts with vendors who handle less sensitive information like contact details. Those vendors present "soft" (and very tempting) targets for hackers since their security tends to be less robust than that of vendors who are accustomed to handling more sensitive information.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075