Issued 4/5/18

Panera Bread Leaked Customer Data on its Website for Months Despite Warnings

Security experts have alleged that US bakery-cafe chain Panera Bread had “millions” of customers’ personal information available and searchable on its site for at least eight months, leaving them vulnerable to identity theft. A plain-text page on Panera’s website revealed the full names, email addresses, physical addresses, phone numbers, date of birth, dietary preferences, and last four digits of credit cards of customers who signed up for the company’s delivery service, the researchers said. The data leak was discovered last year by Dylan Houlihan, who on his LinkedIn page describes himself as the managing principal of New York-based Breaking Bits, a “data mining, reverse engineering and security consulting practice.” In a just-published Medium post with images of old email exchanges, Houlihan stated that he reached out via email, Twitter, and LinkedIn to Panera Bread’s director of information security, Mike Gustavison, upon discovering the breach, but received no reply. In early August, after Houlihan successfully reached him through an introduction, Gustavison said he hadn’t responded to the earlier messages because they were “very suspicious and appeared scam in nature,” according to Houlihan, who added Gustavison then told him that the security team was “working on a resolution.” Months passed without any fix, according to Houlihan. “I have also submitted reports like this to companies, in bug bounties and as a courtesy with no expectation of a reward,” wrote Houlihan. “I have been on

both sides of the table. The response I received is not appropriate whatsoever." Houlihan then contacted Brian Krebs, a security writer and former Washington Post reporter whose blog KrebsOnSecurity is widely read in the industry. A subsequent post by Krebs brought more attention to the problem. Krebs initially placed the number of customers potentially affected by the leak at "higher than 7 million," and later pegged it at 37 million. In statements to Fox Business after Krebs published his piece, Panera's chief information officer John Meister called the issue "resolved" and said that the leaks affected "fewer than 10,000 consumers."