Wells Fargo Does It Again

16 April 2004

In an unpleasant echo of last November's 200,000-customer database compromise, Wells Fargo has once again suffered the theft of a laptop computer containing confidential information for thousands of Wells Fargo customers. What's more, the bank apparently took nearly a month to tell those customers about the theft. A California law, SB 1386, requires companies doing business in the state to "promptly" notify individuals whose personally identifying information may have been affected by a computer database compromise.

While most of those affected by the breach live in Illinois, Indiana, and Colorado, the compromise touched Wells Fargo customers across the United States, including several hundred California residents.

> **"We realize the seriousness of the situation. There certainly is a significant risk associated with this incident."**

The theft occurred on 26 February outside of St. Louis, Missouri, after two Wells Fargo employees stopped their rental car at a gas station convenience store, leaving the yellow Ford Mustang unlocked and the key in the ignition. When they returned from their snackfest, the vehicle was gone. It was recovered five days later stripped of its contents — including the Wells Fargo laptop that had been in the trunk.

Police say there are currently no leads in the case. Wells Fargo will not comment on the status of the investigation.

Incredibly, Wells Fargo failed to notify the customers whose confidential data was stolen until nearly one month after the theft was reported to Edmundson police. A letter that Wells Fargo finally did send on 22 March disclosed only that a Wells Fargo employee's laptop "was stolen from his vehicle's trunk" and that "confidential loan information was stored on the computer's hard drive." The breach was first reported publicly by David Lazarus in the San Francisco Chronicle. To date, Wells Fargo has issued no public statement reporting the incident.

Wells Fargo spokesman Alejandro Hernandez told Identity Theft 911 that the names, addresses, and Social Security numbers of thousands of Wells Fargo mortgage customers were on the stolen laptop. Asked if the total number of customers affected might be even higher — perhaps in the tens or hundreds of thousands — Hernandez repeatedly declined to confirm or deny the possibility.

> **“This is the latest in a long string of cases in which large numbers of people have had their personal information compromised.”**

Hernandez reiterated the statement in Wells Fargo's 22 March letter that "no passwords or personal information numbers were included in the files" on the stolen computer. Reminded that the names, addresses, and Social Security numbers contained on the laptop presented the far more serious threat of new accounts being opened in the victim's name — a crime more difficult to detect, and potentially far more damaging, than the takeover of an existing account — Hernandez replied, "We realize the seriousness of the situation. There certainly is a significant risk associated with this incident." Asked why Wells Fargo chose to downplay that risk in its notification to customers, Hernandez again declined to comment.

Hernandez emphasized that "there is no evidence that the data has been misused," although he also offered no assurances that it had not been misused, or would not be misused in the future. While the computer as a whole was outfitted with standard password protection, he would not say whether or not the data it contained had been encrypted.

Wells Fargo is "still in a leadership role" in developing the forthcoming Identity Theft Assistance Center (ITAC) pilot — a project of the Financial Services Roundtable's BITS division — which Hernandez said is "continuing to move forward" and "will be up and running this year." He noted that Wells Fargo "will be housing the infrastructure" for the pilot project — though presumably not in the trunk of a rented yellow Mustang.

Commenting on the Wells Fargo compromise on behalf of Senator Dianne Feinstein of California, spokesman Scott Gerber said: "This is the latest in a long string of cases in which large numbers of people have had their personal information compromised. It's critical in such cases that businesses and government entities notify consumers that their data has been compromised and that they're at risk for identity theft.

"Senator Feinstein has introduced a bill, now before the Congress, that takes California's SB 1386 as a model, mandating notification of those affected if a database is broken into and personal data compromised. This incident underscores the urgent need for such legislation."

"We apologize sincerely to the customers affected by this incident," said Wells Fargo's Hernandez. "We learned from our experience last November. We hope to learn from this one, too."