

# Almost 600 Accounts Breached in 'Celebgate' Nude Photo Hack, FBI Says

June 10, 2016

By: M. Alex Johnson NBC News

<http://www.cnbc.com/id/102747765>

The stunning leak of nude and intimate photos of scores of celebrities may reach far wider than was previously known, involving the breach of almost 600 online storage accounts, according to unsealed federal court documents.

The "Celebgate" hack resulted in the posting on Aug. 31 of almost 500 purported photos of Hollywood stars, models and other celebrities — including Jennifer Lawrence, Kate Upton, Kirsten Dunst, Kaley Cuoco and U.S. soccer star Hope Solo — to the Wild West-like Internet forum 4chan, from which they quickly spread.

[Apple Inc. confirmed the next day](#) that the photos were obtained through a "targeted attack" on personal information used to maintain storage accounts on its iCloud system. The FBI's Cybercrimes Unit launched an investigation.

As early as October, the investigation began zeroing in on an address on the South Side of Chicago, the FBI said in a search warrant affidavit recently unsealed in U.S. District Court in Chicago.

Using phone records and computer identification information called Internet protocol, or IP, data, investigators found that the compromised accounts were accessed by a single computer linked to two email addresses belonging to Emilio Herrera, 30.

The FBI — which did not say in the affidavit that Herrera is a suspect — said only that the investigation is ongoing.

No other documents have been publicly filed in the case since the affidavit was unsealed, so it isn't known what investigators found at Herrera's home. But in asking for the warrant, the FBI revealed that potentially hundreds — theoretically almost 2,500 — iCloud accounts were targeted. It's important to note that the identification of Herrera — who has no apparent criminal record — doesn't mean he is necessarily a suspect. IP and email addresses can be masked or spoofed through a variety of technologies, and Internet data can be routed through third-party computers without their owners' knowledge using any of a number of software packages.

According to the affidavit, the computer address was successfully used to accessed 572 unique iCloud accounts — each of them an average of about six times. In addition, it said, the computer address was used in almost 5,000 attempts to reset 1,987 other iCloud passwords.

The affidavit doesn't specify whether that number includes multiple attempts to hack the same accounts or whether almost 2,000 individual accounts were targeted. Nor does it say how many of those other attempts were successful.

"A number of them were accounts of celebrities who had photos leaked online," and most of the rest — that is, accounts of people whose photos weren't published — belonged "celebrities, models or their friends and families," according to the affidavit.

Only a handful of alleged victims are identified, and even then only by their initials. They are described as "a female celebrity who has appeared in several movies."

The affidavit tends to support [Apple's insistence at the time](#) that the underlying iCloud technology itself wasn't breached — instead, it indicates that users' account names, passwords and security questions were the means of entry, as Apple contended.

But Apple did [add additional steps to keep hackers out of user accounts](#), and it launched a campaign to encourage users to take stricter security measures.