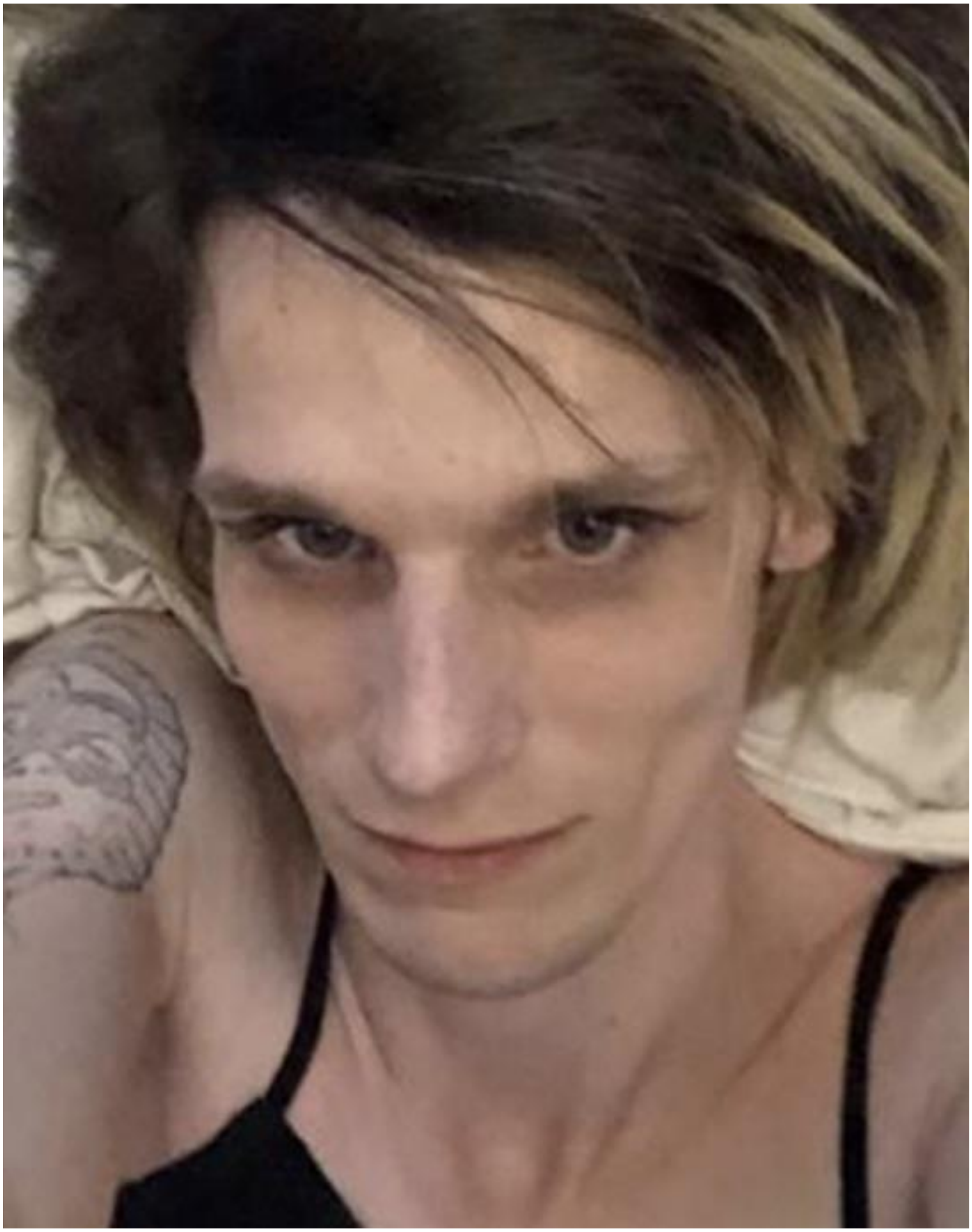
From Data Breach Today:

Capital One: Where Did the Bank Fail on Defense?

Experts Say Bank May Have Made Several Errors

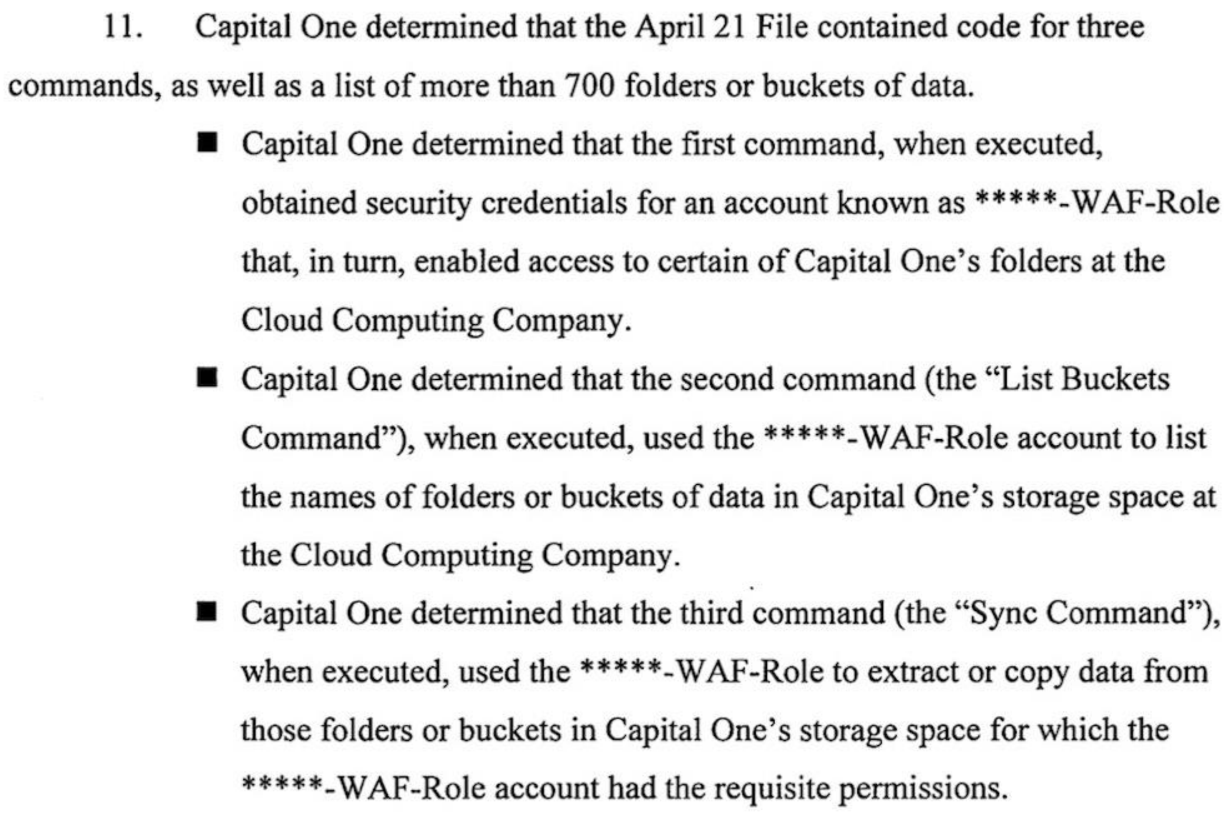
The first question after a major data breach usually is: How did the intruder get in? It's a frustrating query because the answer may not come for months until after an extensive forensics investigation is completed.

But with the Capital One data breach - one of the most extensive breaches of a U.S. financial institution - the answer was surprisingly contained in the criminal complaint.


Paige Thompson

Paige A. Thompson, 33, of Seattle, who is charged with one count of computer fraud and abuse, is alleged to have accessed 100 million credit card applications and a mix of other personal data through a misconfigured firewall (see: *Woman Arrested in Massive Capital One Data Breach*).

Capital One determined that the intruder executed a command that retrieved the security credentials for the administrator account of a web application firewall, according to the complaint, which is based on a sworn statement from an FBI special agent.



11. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.

- Capital One determined that the first command, when executed, obtained security credentials for an account known as *****-WAF-Role that, in turn, enabled access to certain of Capital One's folders at the Cloud Computing Company.
- Capital One determined that the second command (the "List Buckets Command"), when executed, used the *****-WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the Cloud Computing Company.
- Capital One determined that the third command (the "Sync Command"), when executed, used the *****-WAF-Role to extract or copy data from those folders or buckets in Capital One's storage space for which the *****-WAF-Role account had the requisite permissions.

The criminal complaint against Thompson describes how she allegedly accessed Capital One's systems.

From there, Thompson was allegedly able to list the buckets behind the firewall and copy more than 700 folders, which were hosted on Amazon's S3.

But the complaint doesn't address how such a well-resourced organization like Capital One left itself vulnerable to the intrusion and what defensive technologies might have stopped it.

Having more information security resources doesn't necessarily mean better security, says Amit Bareket, co-founder and CEO of Perimeter 81. Large organizations have a much larger attack surface as well, with more corporate resources to monitor, he says.

"This can lead to very simple, yet highly detrimental cybersecurity oversights," Bareket says.

Bypassing the WAF

In theory, an intruder shouldn't be able to skip through a web application firewall and immediately get to sensitive files, says Troy Hunt, a data breach expert and creator of the Have I Been Pwned data breach notification website.

"WAFs are great, but there should be an additional layer of security, and the underlying resources themselves need to be secure," Hunt says. "For argument's sake, if this was lack of authentication on a resource, and they were just relying on the WAF to keep people out, then that is a pretty egregious oversight."

Thompson's resume says she worked for Amazon S3 in Seattle between May 2015 and September 2016. That has led to speculation as to whether her time there aided her ability to carry out the alleged intrusion.

It's possible that Capital One had not regularly refreshed the credentials for the administrator account for the web application firewall, says Brian Vecci, Field CTO with security vendor Varonis. That would be particularly important if Thompson had at one time been an authorized administrator for the firewall.

But the use of the administrator account to access large amounts of data should have been a signal of possible malicious activity for Capital One, Vecci says. Access management is a key part of security, including watching what activities certain accounts undertake, such as copying large amounts of data.

"This means there wasn't the right kind of monitoring in place," Vecci says. "Privileged accounts accessing data this way should be flagged as abnormal."

Hoarding Old Data

Another question is why so much data was not encrypted. Capital One says that some data was encrypted and tokenized, but much wasn't.

One possibility is that the data was indeed encrypted under normal circumstances, but that the administrator account used to access it allowed it to be viewed decrypted, says Ron Burley, head of global security at Instart.

"What seems to have happened is that she was able to get access to an instance running on AWS then use that role to hit the S3 bucket," Burley says. "If she did this through an IAM [system], her access level would have piggy-backed her access to the data as well. That would include the keys needed to decrypt data, making any encryption moot."

Hunt says a more relevant question is why Capital One still needed credit card application data from as long as 14 years ago. The personal data covered 100 million people and was collected between 2005 and early this year.

The data includes applicant names, addresses, birth dates, credit histories, balances and payment histories. The prevailing wisdom these days is that organizations shouldn't hold onto data that's unneeded.

That is codified in Europe's General Data Protection Regulation, which says organizations should generally delete personal data when it's no longer needed for the purpose it was collected, such as if someone closes their account.

But Hunt says "organizations tend to look at data as an asset, and they don't ever look at it as a liability."

And Vecci adds: "When it comes to file data security, people don't delete anything, and that is a problem. It was a problem in the Sony breach, and it's a problem now."