Exhibit 99.1

Investor Relations Contact
United States
Jeff Norris
(703) 720-3171
Jeff.Norris@CapitalOne.com

Danielle Dietz
(703) 720-2463
Danielle.Dietz@CapitalOne.com

Media Contacts
United States
Tatiana Stead
(703) 720-2352
Tatiana.Stead@CapitalOne.com

Sie Soheili
(703) 720-3929
Sie.Soheili@CapitalOne.com

Canada
Suma Boby
(905) 599-1434
Suma.Boby@CapitalOne.com

Capital One Announces Data Security Incident

Perpetrator Arrested by Federal Law Enforcement

MCLEAN, Va., July 29, 2019 /PRNewswire/ -- Capital One Financial Corporation (NYSE: COF) announced today that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.

Capital One immediately fixed the configuration vulnerability that this individual exploited and promptly began working with federal law enforcement. The FBI has arrested the person responsible and that person is in custody. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.

"While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened," said Richard D. Fairbank, Chairman and CEO. "I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right."

Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.

Importantly, no credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised.

The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:

- Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information
- Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018

No bank account numbers or Social Security numbers were compromised, other than:

- About 140,000 Social Security numbers of our credit card customers
- About 80,000 linked bank account numbers of our secured credit card customers

For our Canadian credit card customers, approximately 1 million Social Insurance Numbers were compromised in this incident.

We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.

Safeguarding our customers' information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.

We are very thankful to the FBI's Seattle Field Office and Special Agent Joel Martini, to U.S. Attorney Brian T. Moran, and to Assistant U.S. Attorneys Steven Masada and Andrew Friedman of the Western District of Washington for the speed with which they responded to this incident and apprehended the responsible party.

For more information about this incident and what Capital One is doing to respond, visit www.capitalone.com/facts2019. In Canada, information can be found at www.capitalone.ca/facts2019 and www.capitalone.ca/facts2019/fr. The investigation is ongoing and analysis is subject to change. As we learn more, we will update these websites to provide additional information.

Answers to certain questions related to the cybersecurity incident follow.

What was the vulnerability that led to this incident?
We believe that a highly sophisticated individual was able to exploit a specific configuration vulnerability in our infrastructure. When this was discovered, we immediately addressed the configuration vulnerability and verified there are no other instances in our environment. Among other things, we also augmented our routine automated scanning to look for this issue on a continuous basis.

How did you discover the incident?
Like many companies, we have a responsible disclosure program which provides an avenue for ethical security researchers to report vulnerabilities directly to us. The configuration vulnerability was reported to us by an external security researcher through our Responsible Disclosure Program on July 17, 2019. We then began our own internal investigation, leading to the July 19, 2019, discovery of the incident.

When did this occur?
On July 19, 2019, we determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for credit card products and Capital One credit card customers. This occurred on March 22 and 23, 2019.

Was the data encrypted and/or tokenized?
We encrypt our data as a standard. Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of data.

However, it is also our practice to tokenize select data fields, most notably Social Security numbers and account numbers. Tokenization involves the substitution of the sensitive field with a cryptographically generated replacement. The method and keys to unlock the tokenized fields are different from those used to encrypt the data. Tokenized data remained protected.

Did this vulnerability arise because you operate on the cloud?
This type of vulnerability is not specific to the cloud. The elements of infrastructure involved are common to both cloud and on-premises data center environments.

The speed with which we were able to diagnose and fix this vulnerability, and determine its impact, was enabled by our cloud operating model.

What are the expected financial impacts of the incident?
We expect the incident to generate incremental costs of approximately $100 to $150 million in 2019. Expected costs are largely driven by customer notifications, credit monitoring, technology costs, and legal support. We expect to accrue the costs for customer notification and credit monitoring in 2019. The expected incremental costs related to the incident will be separately reported as an adjusting item as it relates to the Company's financial results.

For years we have invested heavily in cybersecurity and we will continue to do so. Beyond the adjusting item in 2019, we expect any incremental investments in cybersecurity to be funded within our current budget.

The Company carries insurance to cover certain costs associated with a cyber risk event. This insurance is subject to a $10 million deductible and standard exclusions and carries a total coverage limit of $400 million. The timing of recognition of costs may differ from the timing of recognition of any insurance reimbursement. Gains on insurance recoveries associated with the incident will also be treated as an adjusting item as it relates to the Company's financial results.

The Company is affirming its existing efficiency guidance, which in all cases is net of adjustments. The Company expects to achieve modest improvement in 2019 annual operating efficiency ratio compared to the 2018 annual operating efficiency ratio. Relative to 2019, the Company also continues to expect modest improvement in 2020 annual operating efficiency ratio. And the Company continues to expect annual operating efficiency ratio to be 42 percent in 2021. The Company continues to expect that improvements in operating efficiency ratio will also drive significant improvement in annual total efficiency ratio in 2021.

Cautionary Statements Regarding Forward-Looking Statements

This document contains forward-looking statements, which involve a number of risks and uncertainties. All statements that address operating performance, events or developments that we expect or anticipate will occur in the future, including those relating to operating results and the cybersecurity incident we announced on July 29, 2019, are forward-looking statements. The Company cautions readers that any forward-looking information is not a guarantee of future performance and that actual results could differ materially from those contained in the forward-looking information due to a number of factors, including those listed from time to time in reports that the Company files with the Securities and Exchange Commission, including, but not limited to, the Annual Report on Form 10-K for the year ended December 31, 2018.

About Capital One

Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N.A., had $254.5 billion in deposits and $373.6 billion in total assets as of June 30, 2019. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches located primarily in New York, Louisiana, Texas, Maryland, Virginia, New Jersey and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

# # #