Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Revising Cloud Contracts In Light Of Capital One Cyberattack

By **Nicholas Smith and Rita Ganguli** (October 11, 2019, 1:58 PM EDT)

Nicholas Smith

Rita Ganguli

On July 30, Capital One Financial Corp., the fifth largest U.S. credit card issuer, reported that approximately 106 million card customers' and applicants' personal information was stolen by a hacker in late March.

The breach implicated 140,000 Social Security numbers and 80,000 bank account numbers, as well as credit scores, payment histories and credit limits of individuals associated with Capital One. The stolen data was stored on the Amazon Web Services Inc. cloud and, according to Capital One, was stolen via a misconfigured firewall on an AWS bucket (i.e., a cloud server used to store sensitive information).

Because its security defenses did not detect it, Capital One was not alerted of the intrusion until July 17 — almost four months later — when a third party notified Capital One of the attack. Recent federal investigations identified the hacker as a former employee of AWS.

Amazon.com Inc. wholly refused blame for the data breach. According to Amazon, although it hosted Capital One's data, the software targeted by the hack was managed by Capital One itself. Amazon asserted that the software "was not compromised in any way and functioned as designed" and that the hacker gained access through "a misconfiguration of the web application and not the underlying cloud-based infrastructure." Amazon also stressed that its cloud clients have full ownership of and control over the manner in which their data is stored, secured and protected and that Amazon offers "sophisticated technical and physical controls" that are designed to help combat any unauthorized access.

This recent breach is particularly notable because Capital One was one of the first large financial institutions to move its systems to cloud computing. Capital One functioned like a "proof of concept" for regulators looking to see if migration to the cloud could be done securely. In December 2018, Rob Alexander, Capital One's chief information officer, announced that "we are entirely focused on moving to the public cloud."

Unfortunately, Capital One is not alone in being the target of a successful cyberattack. Indeed, cyberattacks have recently become fairly routine events. In 2019 alone, there have been 3,494 successful, known cyberattacks against financial institutions. On a typical day, institutions like

Mastercard Inc. combat an estimated 460,000 intrusion attempts, up 70% from 2018. Associated costs can accrue rapidly: the average cost of a security breach in the U.S. escalated recently to $8.2 million. These costs can arise from everything from regulator fines to class action lawsuits, and do not include the reputational harm that can result from these often very public events.

Cloud Providers Fly Under the Radar

The major cloud platform services providers (i.e., AWS, Microsoft (Azure), and Google Cloud) have historically kept details of their internal security protocols largely hidden from financial institutions that wish to enter into services contracts. Nevertheless, technology companies such as these are now crucial players in the U.S. banking system.

And as highly regulated entities, banks must be able to understand the infrastructure that is being used within their respective businesses, especially if such banks contemplate relying on third-party cloud providers or if vendors use such providers to host bank data. This regulatory mandate toward openness is in direct tension with the corporate culture of Silicon Valley, where transparency of this sort is seen as revealing crucial competitive advantages.

This culture clash is coming to a head. Our view is that a corporate cultural tendency toward opacity cannot endure when banks are being held to industrywide standards for risk management and operational resilience.

While regulators wield substantial influence over banks, they only have limited power over nonbanks and typically rely on banks to vet their own non-bank vendors. The U.S. Department of the Treasury reported last year that bank regulators had not "sufficiently modernized to accommodate cloud and other innovative technologies." Thus, since their inception, technology companies, such as the most prominent cloud platform providers, have flown under the radar of federal regulators.

Cloud service providers have also been actively engaged in political efforts to preserve their preferred approach in the face of mounting regulatory pressure. As recently as 2017, government efforts to consider proposed new cybersecurity standards stalled out, due in part to pressure by cloud service providers. The industry's justification for its position was that cloud companies simply sell a system and turn over the job of running and securing the system to their clients, and that imposing additional cybersecurity requirements could unnecessarily lead to redundancy and increases in compliance costs while leaving systemically important financial institutions less secure.

The mood in the industry and its regulators seems to be shifting, though, in the wake of the Capital One incident. While the Capital One breach was determined to have resulted from Capital One's error rather than an AWS' vulnerability, initial reports suggested that AWS itself had been breached, setting off rounds of discussions of systemic risk and what Capital One could realistically achieve vis a vis AWS given typical customer cloud platform service agreement terms.

Stepping back from this specific incident, it realistically is a matter of when, not if, a cloud platform service provider will suffer a cybersecurity incident. With that concern now at the front of mind, transparency and coordination are increasingly pressing issues for both regulators and financial institutions, and regulators are beginning to take action. In response to the Capital One breach, the Federal Reserve began an official investigation of an Amazon facility in Virginia on Aug. 1, the first of what may be ongoing oversight of cloud providers that have become repositories of sensitive banking information.

A number of regulators and industry figures with quasi-regulatory influence have also taken recent action to increase cybersecurity requirements for financial institutions that will, in turn, impact the relationship between financial institutions and their service providers. For example, on Oct. 8, the Deposit Trust Co., the Fixed Income Clearing Corp., and the National Securities Clearing Corp. all filed notice of proposed changes to their cybersecurity rules.

How Contractual Provisions Can Mitigate Risk

Until some form of regulatory action breaks the stalemate between financial institutions and their cloud providers, financial institutions are in the position of looking to their contracts with cloud providers to identify and to attempt to address potential risks. In our view, the issues below are some that are particularly worthy of reconsideration:

Liability

Liability provisions should lessen the risk of significant irrecoverable loss and should allow a financial institution to engage in active management when service performance is at risk. Typical cloud service contracts greatly limit the circumstances in which the cloud provider would be liable at all under the agreement for cybersecurity incidents, and typically limit such liability in the same manner other liability is limited.

While cloud platform providers have to date been able to hold to lower limits of liability than is often agreed in services agreements for traditional, bespoke information technology outsourcing services, as banks move more and more of their critical systems into the cloud, banks should press for the limits of liability to move away from the cloud providers' historic practice and comfort levels and should instead turn more on the risk to the bank if there is a major service failure.

Security

Security provisions should be clear and set a high standard. The default position of cloud providers to date is that such providers will set and comply with their security standards and that they will provide customers limited information regarding what, exactly, those standards are (and whether those standards are followed).

A few suggestions for contractual provisions regarding this issue include:

- Seek provisions making the cloud provider responsible for ongoing legal compliance, including specific standards such as the Federal Reserve Board and Office of the Comptroller of the Currency risk- management guidelines and New York State Department of Financial Services Part 500;

- Require a business continuity management plan to be tested and updated regularly, and for the results of those tests to be shared with the customer;

- Require the provider to conduct penetration testing and share the results with the customer as a part of the engagement;

- Require the cloud provider to provide the customer notice of material changes in security procedures so that the customer is apprised of its security posture on an ongoing basis; and

- Consider enhanced termination rights and financial remedies (e.g., break fees or reimbursement of certain costs) if the cloud provider implements security changes without appropriate notice to the financial institution

Audit

The default position of cloud providers is generally that they will conduct audits and not allow third parties to have access to such providers' systems. Disclosure to customers regarding the results of such audits is also limited.

While the position that a cloud provider will not allow access to third parties to conduct security audits is nonnegotiable both for security reasons and as a practical matter (the one-to-many service model makes it totally unworkable for a cloud provider to grant that sort of access to any one customer), financial institutions should pursue greater transparency given the substantial regulatory oversight to which they are subject.

Cyber Event Notification Requirements

A vendor security breach can start the clock on a financial institution's legal requirement to notify its regulators and affected individuals. Cloud providers have been very resistant to specific timing requirements for notifying customers about security breaches, preferring language like "reasonable timeframe" and vigorously resisting a contractual 24-hour notification requirement that is considered good industry practice for other IT service providers.

The costs and regulatory exposure that may result from any delay in breach notification present material risk to financial institutions; accordingly, cyber event notification provisions should be given renewed emphasis by financial institutions in their negotiations with cloud providers.

Nicholas Smith is a partner, and Rita Ganguli is an associate at Milbank LLP.