Keeping Data-Breach Reports Confidential After Capital One

By **John Reed Stark** (June 29, 2020, 5:08 PM EDT)

John Reed Stark

When U.S. Magistrate Judge John Anderson ordered[1] Capital One Financial Corp. to turn over a post-breach digital forensics report to the consumer plaintiffs in the multidistrict litigation relating to the bank's July 29, 2019, data breach,[2] the decision sent shock waves through the community of legal and forensic firms that help companies respond to cyberattacks.

Now, with U.S. District Judge Anthony Trenga's June 25 order denying Capital One's motion for reconsideration,[3] the shock waves continue.

In the case of In re: Capital One Customer Data Security Breach Litigation, pending in the U.S. District Court for the Eastern District of Virginia, Capital One contended that the report, drafted by Mandiant and commissioned and supervised by Capital One's outside counsel, helped counsel develop its legal theories about the cyber incident and formulate strategy for defending against the inevitable ensuing litigation. Therefore, the Mandiant report constituted attorney work product and was protected from discovery during litigation.

But consumer plaintiffs disagreed, arguing that because Capital One had previously engaged Mandiant on an ongoing retainer basis, Mandiant would have delivered the report to Capital One without litigation looming. Therefore, the Mandiant report did not qualify as attorney work product and was subject to routine discovery.

This situation represents yet another emerging challenge in the aftermath of a data breach. On the one hand, companies that experience data breaches and their legal teams need to seek truth and, thus, pay for a digital forensic report that offers a robust, objective and unmerciful investigation of a data security incident.

This allows the company not only to insure proper regulatory and consumer notifications and prepare for inevitable class action litigation but also to initiate effective remediation and to strengthen future cyber-defensive efforts.

But on the other hand, post-breach digital forensic reports can detail the good, the bad and the ugly of a company's cybersecurity infrastructure and governance, and can be shrewdly weaponized by class action lawyers.

Judges will always consider the issue of work product and post-breach digital forensic reports on a fact-intensive case-by-case basis.

Thus, it is also important to consider the Capital One decision not in a vacuum, but in context with a handful of other federal court cases, including decisions relating to data breaches at: Experian PLC,[4] Premera BlueCross,[5] Dominion Dental,[6] Marriott International Inc.,[7] Arby's Restaurant Group Inc.,[8] Target Corp.,[9] Genesco Inc.[10] and Albertsons Companies Inc.[11]

Taken together, lessons gleaned from these cases allow for a more pragmatic perspective.[12]

This article offers some alternatives concerning forensic firm engagement after a breach, together with some added guidance and considerations for the road ahead.

Starting Anew

In light of the Capital One decision, some have recommended that in the event of a cyberattack, a company should essentially start anew, and ensure that outside counsel retains a cybersecurity vendor with which the company has no preexisting relationship.

This likely entails hiring two digital forensic firms with two distinct functions — one for mitigation, where reports can be shared with regulators, auditors, etc., and one for litigation, where reports are kept confidential. This option might very well be best practice, but it can also be cost-prohibitive and unworkable for some companies.

Imagine that you have a history of heart disease in your family, so you hire a cardiologist each quarter to undergo various testing and to discuss the best exercise, diet and other steps to stay healthy. Naturally, the relationship with your cardiologist grows in familiarity, importance and confidence.

Now imagine that you suddenly suffer a heart attack but are told to stay away from your trusted cardiologist and instead engage an entirely new cardiologist to help recover from the heart attack. Of course, this makes absolutely no sense — but helps puts into context such an extreme interpretation of the Capital One decision.

First off, expert digital forensics firms are few and far between and, like plumbers after a hurricane, are already overextended. Amid the early bedlam of a data breach, it can sometimes take weeks or even longer to successfully engage a digital forensics firm, which ironically could provide ideal fodder for plaintiffs to exploit as evidence of a company's sluggish breach response and remediation efforts.

Moreover, the Capital One decision does not necessarily mandate the sacrificial and exorbitant reinventing of the wheel with a new forensic firm after a breach. In his June 25 order,[13] Judge Trenga emphasizes that victim companies who already have a retained a digital forensic firm need not necessarily engage an additional firm.

Judge Trenga clearly appreciates that data breach investigation reports are a distinct form of communication between companies and their cybersecurity consultants, and that a company's data breach investigation process can "look and feel different than typical operations with a managed security provider." Judge Trenga states in a footnote:

Capital One contends that the Order "incentivizes companies to either (a) forego keeping an incident response vendor on retainer or (b) hire a new, unfamiliar vendor to investigate any incident from which litigation is expected to result. ... But that contention ignores the alternatives available to produce and protect work product, either through different vendors, different scopes of work and/or different investigation teams.[14]

Just the Facts

There exists no standard format, structure or other organizational model for post-breach digital forensic reports.

Thus, instead of a post-breach report, direct the engaged forensic firm to draft a letter to the law firm laying out a summary of nonprivileged factual findings. The letter could

include: the names and characteristics of any indicators of compromise; a discussion of any remnants, artifacts or fragments of any files left by the attacker; and log evaluations and other factual findings and details.

The letter should not contain conclusions relating to exfiltration, attribution or even precise parameters of the attack vector — those subjects can be covered during oral discussions.

Forensics investigators should be instructed not to speculate. Nor should the letter's language convey judgments — whether legal or based on recognized industry standards. This approach actually makes sense. Often the subject of intense debate, subjective opinions, assumptions, and —always meticulously qualified — conclusions relating to a cyberattack are better suited for oral read-outs rather than the written word.

Roll the Dice

Admittedly, by engaging a previously retained forensics firm to respond to a new data breach, a victim-company is taking on risk. Judges now routinely take a hard look at what were historically considered sacrosanct and well-settled issues of the attorney-client relationship.

But with certain precautions and some thoughtful and careful deliberation at the threshold, outside counsel can hire a company's trusted retained forensics firm to conduct a data breach investigation but still avoid the fate of Capital One. Counsel should:

- Draft appropriate incident-specific engagement documentation explaining that any new work performed by the forensics firm would not have been prepared in substantially similar form without the threat of litigation. The nature and scope of work should be distinct from generalized ongoing services and customized solely to manage the new breach.

- Take actions that evidence that the forensics firm's investigation, and its report, were produced and disseminated for the purpose of legal defense and not for business operations or regulatory compliance.

- Modify any existing statement of work to provide that the new work is to be performed solely at the request and direction of counsel — and describe in detail the work to be done for legal purposes. Avoid using boilerplate statements of work from forensic firm engagement letters and retainer agreements.

- Document expenditures to demonstrate that work is clearly being performed with outside counsel for a legal purpose in anticipation of litigation and not for a business purpose. If possible, billing should be made to a company's legal department and not its IT department.

- Ensure that the forensic firm communicates directly and only with counsel in a consistent, secure and confidential manner, and design effective communication protocols and procedures.

- Engage any other nonlitigation work — such as future penetration testing or remediation projects — in a separate and distinct statement of work.

- Use a different investigation team than the previously retained commercial team. The investigation team could review historical reports and perhaps meet with

commercial team members to understand the work completed under the commercial terms, but information flow between the two teams should be a one-way street.

- Insist that the forensic firm conduct its investigation based on documentation that can be provided to an adverse party for an independent investigation. Given that work product protection can be overcome by a finding of substantial need by the adverse party, this kind of preparation establishes a defense against such an assertion.[15]

Skip Drafting a Report

If a digital forensics report is not specifically required by contract or law, companies should consider eschewing the drafting of a forensic report altogether.

Sometimes digital forensic reports offer the most thorough, comprehensive and authoritative analysis of a cyberattack. But sometimes reports contain conjecture, hypothesizing, speculation, supposition and simple old-fashioned guesswork. Here's why.

While some data security incidents may provide key evidence early on, most never do, or even worse, provide a series of false positives and other initial stumbling blocks. After a cyberattack, malware reverse engineers rarely, if ever, discover a "CSI"-like evidentiary trail.

Digital forensic evidence of a data security incident is rarely in plain view; it can rest among disparate logs (if they even exist), volatile memory captures, server images, system registry entries, spoofed IP addresses, snarled network traffic, haphazard and uncorrelated timestamps, Internet addresses, computer tags, malicious file names, system registry data, user account names, network protocols and a range of other suspicious activity.

Evidence can also become difficult to nail down — logs are destroyed or overwritten in the course of business; archives become corrupted; hardware is repurposed; and the list goes on.

Criminal defense lawyers conducting internal investigations of wrongdoing — from insider trading and employee theft to financial reporting fraud and money laundering — are notorious for avoiding written reports. After all, aside from being extraordinarily expensive, written investigative reports not only invite litigation, they can also cause unnecessary confusion and management drag.

Best Practices Regarding a Forensic Report's Distribution

Courts have consistently recognized that post-production disclosures are appropriately probative of the purposes for which the work product was initially produced.[16] When post-breach digital forensic reports are shared for business and regulatory purposes, as opposed to legal or litigation-related purposes, the risk of losing work product protections can increase significantly.[17]

No matter which engagement option is pursued, counsel should design a strategy about with whom, internally and externally, incident response work is discussed and shared, limiting the report's distribution and taking steps to ensure that anyone who receives the report does not use it for business purposes. However, limiting the distribution of a post-breach report is a lot easier said than done and this process will inevitably become mired

with complications both externally and internally.

Internal parties wanting the report may include: a parent company, the board and its audit committee, the in-house incident response team, the IT department and even employee unions that are concerned about exfiltation of employee information.

Meanwhile, external parties that will seek copies include: insurance carriers, external auditors, affiliate companies, outside vendors that have been impacted by the breach (which may have contracts that require a sharing of the report), key customers — especially on government contracts, shareholders and other stakeholders — who may threaten financial or economic retaliation if not included on distribution lists — and an array of state and federal regulatory agencies.

Saying no to requests from regulators, auditors, key vendors, critical customers and other crucial internal and external constituencies can have bet-the-company consequences. Thus, counsel should establish; strict and methodical procedures for recipient selection; centralized decision-making and record-keeping processes for any exceptions; and a carefully drafted script for any oral briefings limited to only factual findings.

If distribution is absolutely necessary, carefully document the process, make redactions, sign confidentiality and common interest agreements,[18] implement strict governance and technological safeguards to deter unauthorized circulation by recipients, and, if possible, omit from distribution the underlying investigative materials and any citations or references thereto.

Looking Ahead

A strict interpretation of the Capital One decision — i.e., replacing a previously engaged data breach response firm with a new one after a data breach — is only one alternative. There exist other options that do not undermine a central tenet of good cyber hygiene — being ready to respond rapidly to data breaches by preselecting an expert data breach response firm to stand by on retainer.

My take is that when a company like Capital One does the right thing by engaging a top-notch forensic firm to stand by in the event of a data breach, their keen and responsible preparation should be celebrated and not rebuked. Period. End of story.

John Reed Stark is president of John Reed Stark Consulting LLC. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as chief of its Office of Internet Enforcement.

[1] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/05/CapOne-Mandiant-Report-Decision.pdf.

[2] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/05/CapOne-Mandiant-Report-Decision.pdf.

[3] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/CapitalOneOrder2.pdf.

[4] https://www.datasecuritylawjournal.com/files/2017/05/Experian-Order-Denying-Plaintiffs-Motion-to-Compel.pdf.

[5] https://www.leagle.com/decision/infdco20171030l11.

[6] https://dockets.justia.com/docket/virginia/vaedce/1:2019cv01050/451226.

[7] https://www.johnreedstark.com/wp-content/uploads/sites/180/2019/09/1194000-1194859-https-ecf-mdd-uscourts-gov-doc1-093110535843.pdf.

[8] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/gand-1_2017-mi-55555-00453.pdf.

[9] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/Target-Decision2-1.pdf.

[10] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/Genesco-order-applying-privilege-1.pdf.

[11] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/Albersons-Order.pdf.

[12] "Data Breach Forensic Reports: Keeping a Grail Document Confidential," by John Reed Stark, (D&O Diary, June 16, 2020) at https://www.dandodiary.com/2020/06/articles/cyber-liability/guest-post-data-breach-forensic-reports-keeping-a-grail-document-confidential/.

[13] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/CapitalOneOrder2.pdf.

[14] Judge Trenga's decision can be found at https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/CapitalOneOrder2.pdf.

[15] https://sterlingmiller2014.wordpress.com/2019/06/05/ten-things-a-primer-on-the-work-product-privilege/.

[16] Cf. In re Experian Data Breach Litig., 2017 WL 4325583, at *2 ("If the report was more relevant to Experian's internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation, then the full report would have been given to that team.").

[17] Leibovic v. United Shore Financial Services, LLC, 2017 WL 3704376 (E.D. Mich. Aug. 28, 2017) at https://casetext.com/case/leibovic-v-united-shore-fin-servs-llc?resultsNav=false (aff'd in In re United Shore Fin. Servs., LLC, No. 17-2290, 2018 BL 1881 (6th Cir. Jan. 03, 2018) at https://www.pbwt.com/content/uploads/2018/01/Doc-4.pdf).

[18] In contrast to attorney-client privilege, work product protection is not automatically waived by disclosure to a third party. To determine whether work product protection is waived, most courts distinguish between disclosures to an adversary versus a

nonadversary. For example, in the Experian data breach litigation, Judge Guilford noted that forensic reports may be disclosed to third parties so long as the disclosure is "consistent with maintaining the secrecy against opponents."https://www.datasecuritylawjournal.com/files/2017/05/Experian-Order-Denying-Plaintiffs-Motion-to-Compel.pdf.