So, CrowdStrike Happened. Do You Have Any Claims? Or Any Liability?

Paul Poirot
ppoirot@blegalgroup.com
646-374-0025

While the CrowdStrike Falcon update incident on July 19, 2024 caused initial turmoil and profound problems for some industries (notably airlines), many institutions were spared the full effects of the disruption. Those institutions that successfully mitigated the impact had robust business continuity/disaster recovery ("**BC/DR**") plans that allowed them to quickly and effectively rollback to pre-update backups of their Falcon instances while they awaited a patch from CrowdStrike.

After initial reports of the problems from Europe and the UK, institutions in the United States and other parts of the world had the luxury of a relatively fast confirmation from CrowdStrike that the errors were caused by a problem with CrowdStrike's own update and were not the result of an attack by a malicious actor. The financial industry in particular also benefitted from the timing of the incident: a Friday in July close to the middle of the month, but after the end of many payroll periods. Simply put, things were slower and more manageable than they might have been at other times.

Still, there are important lessons to be learned by legal teams, and they should consider conducting post-mortems with their IT and information security ("**IT/IS**") teams as the dust settles from the incident. So, before you cash in that $10 Uber Eats voucher CrowdStrike sent, consider what real remedies your organization might have.[1]

Privity and Vendors

As a preliminary matter, many of the topics discussed below will depend on your organization being in privity with CrowdStrike (i.e., your organization contracts directly with CrowdStrike and your organization experienced a material adverse effect from the incident). Most sophisticated tech vendors like CrowdStrike disclaim third party beneficiaries to their agreements. So, if your organization faced an outage as the result of a vendor to your organization being down, your only claim(s) may be against that vendor and not directly against CrowdStrike. (Conversely, that vendor may have a direct claim against CrowdStrike.)

What's Our Best Shot?

The most likely remedy for most organizations will arise from breach of guaranteed service levels by either CrowdStrike (for your organization's instance of Falcon) or your other vendors. Because of the widespread effect of the outage and public awareness of why and how it happened, some organizations may be overlooking that their vendors (including CrowdStrike) have guaranteed service levels. Be sure that your IT/IS teams are tallying up the

[1] This note does not constitute legal advice or the provision of legal services. It is for general informational purposes only. Before proceeding with any actions, please review your organization's agreements that might affect a claim against CrowdStrike or any other parties and discuss with your Bortstein Legal Group attorney.

downtime of your Falcon instance and the downtimes of your vendors, and not just writing it off to "everyone was down." These service level remedies will also incentivize vendors to make claims directly against CrowdStrike, which will incentivize CrowdStrike to ensure that this doesn't happen again.

This incident is a good reminder of the importance of service level guarantees in your agreements. Customers of tech companies are all too often willing to simply accept form service level terms, or fail to review them. These guarantees, their triggers, and any compensation should be carefully reviewed and negotiated in every agreement. Your Bortstein Legal Group attorney can assist with this review, bringing to bear industry experience and knowledge of market standards.

What's Good for the Goose….

If your organization provides services to others, be prepared for your clients to make their own service level claims against you. Compensation (often credits) for breach of service level guarantees may be due as soon as the next calendar month, although parties sometimes negotiate terms for quarterly or even annual reconciliation. Depending on the exposure of your organization, this compensation could materially affect revenue streams.

Your organization may be considering pre-emptively offering compensation to your clients (perhaps not those Uber Eat gift cards we mentioned earlier…). If your organization goes that route, as legal counsel you need to understand if the compensation is intended as a bonus to clients to restore trust and solidify relationships, or it is offered in lieu of the compensation required under your agreements. If the latter, be sure to properly draft the terms of the offer to ensure that accepting the compensation waives any additional claims.

Can We Go Big?

Depending on the terms of your agreement, your organization may have a claim against a warranty that CrowdStrike's software will be error-free or that it will be suitable for use. However, most tech vendors limit remedies around errors to correcting such errors and disclaim standard implied warranties of merchantability or fitness for a particular purpose. This may be the situation with your organization's agreement directly with CrowdStrike.

That said, this may be a case where having a vendor between your organization and CrowdStrike plays to your advantage. You may have negotiated more favorable terms with a smaller vendor than you might have if you contracted directly with CrowdStrike: your organization might have a more robust claim that your vendor's product or service is provided error-free or perhaps the vendor did not disclaim relevant warranties. You will still want to carefully weigh the value of such a claim, as enforcement might require you to sue your vendor. Depending on your leverage with the vendor, a better course might be a timely call to a sales rep and an open-ended "how do you want to make this right?" question. Your Bortstein Legal Group attorney can help you consider your options and possibly strategies.

Wait. Is this On Us? On Our Vendors?

You will want to review with your IT/IS teams what the incident revealed about your team's ability to rollback your CrowdStrike Falcon instance, as well as assess the promptness and thoroughness of notifications sent to clients and customers (and received from your vendors and subcontractors) regarding the impact of the incident on products and services. Because the incident does not appear to have been malicious, contracting provisions around security incidents probably do not apply; however, the incident should have triggered well-drafted BC/DR provisions for your organization and your vendors. If yours was one of the lucky organizations that was not seriously affected by the outage, the incident might have provided the opportunity for an unplanned test of your BC/DR plans. The unplanned nature might have revealed areas for review by your IT/IS team that scheduled tabletop exercises do not.

If your organization provides services or products to others, you will want to confirm that your organization met its obligations to notify your customers and clients under the BC/DR obligations in your agreements. Similarly, you will want to review how your vendors performed. Make sure (in both directions) that IT on one side didn't just instant message IT on the other side with a quick "we're down bc of CS."

In addition to the service level claims discussed earlier, factors you might need to consider when reviewing agreements in one direction for the response of your organization, and in the other director the response(s) of your vendors and sub-contractors, include:

- What are the triggering criteria of BC/DR obligations?
- Did everyone provide notice through the proper channel(s)? Was there sufficient detail and information in the notice(s)?
- What is the nature and necessary timing of notifications?
- What constituted an "all clear" after the incident and was it properly communicated?
- Do your IT/IS teams now find all of these criteria to be appropriate, or should you consider new best practices and preferred contracting provisions? Provided by your organization? Received from your vendors and subcontractors?

If it's time to update the BC/DR terms in your organization's agreements, reach out to your Bortstein Legal Group attorney for assistance.

Notifications to CrowdStrike

If your organization was directly affected by the incident and is in privity with CrowdStrike, you should carefully review your agreements with CrowdStrike to determine what recourse your organization might have against CrowdStrike, as well as what notice you must provide to protect that claim.

But Don't We Have Insurance?

A caveat to all of this might be claims against business continuity insurance or cyber-insurance. Those policies are usually very specific to individual entities, so you will want to review the terms, calculate deductibles, and speak to your insurer(s).

Damages that Could Have Been

Unfortunately, even if your organization is in contractual privity with CrowdStrike, most of the downstream damages within your organization probably won't be recoverable against CrowdStrike. Most tech vendors, like CrowdStrike, will exclude things like lost profits, lost business opportunities, or special, incidental, indirect, or consequential damages. In other words, the lost transaction fees for your credit card unit likely are not recoverable if those losses were due to point-of-sales computers being down at commercial retailers.

* * *

If you have any questions about the topics discussed, please reach out to your Bortstein Legal Group attorney or Paul Poirot at ppoirot@blegalgroup.com.