Lowenstein Sandler's Cybersecurity Awareness Series
Session 8 – Cyber Breaches in M&A Transactions

By Marita A. Makinen and Ken Fishkin
DECEMBER 2022

Ken Fishkin: Welcome to another edition of Lowenstein Sandler's Cybersecurity Awareness series. I'm Ken Fishkin, the Information Security Manager here at Lowenstein Sander and with me today is Marita Makinen, our chair of our M&A practice.

I want to discuss an issue that related to both a cyber breach and an M&A transaction, and it dealt with CafePress. Back in 2019, they had a big major breach that involved thousands of unencrypted Social Security numbers, partial credit card payment numbers, and millions of email addresses and passwords that were stolen, and the company decided not to report it. Unfortunately, the news reported it seven months later, so they were forced to report it as well.

Unfortunately, as a result of this breach, the company did nothing to correct its security posture. Some time went by, and the company got acquired by a new company, and the new company decided not to do anything to improve the company's cybersecurity posture as well. And as a result of all that, back in March of this year, a judgment was made against both the old company and the new company, because neither company was able to fix the security issues that the FTC identified.

Marita, do you have anything that you would like to comment about this case?

Marita A. Makinen: Sure. I think first, it's important to understand the legal framework in which the CafePress issues arose. It's very difficult for companies, especially smaller companies, to be able to comply with all of the different privacy and data security laws that are in effect now—both US, federal, state laws, international laws.

In the case of CafePress, the FTC brought the action enforcement action against the company, and the FTC is traditionally involved in enforcing laws relating to false advertising. In addition, when there is a data breach, companies sometimes don't tell the truth about it, or they don't give customers all of the information that they need. So, if that happens, the FTC may bring an action against that company saying that they've violated the false

advertising laws. Even beyond that, the CafePress case could have given rise to issues under state laws. Almost all of the states have laws that govern who needs to be notified when there's a data breach. Some states even have their own freestanding privacy laws. So, a company could potentially face liabilities under more than one set of laws if there is a data breach.

Why is this important in the context of M&A? CafePress involved in an M&A transaction, and both the seller and buyer were pursued by the FTC, and both of them had to take remedial actions, and in the case of the seller, they had to pay a fine. First of all, it's important to understand that in an M&A transaction, the buyer generally takes on the liabilities of the business—whether it's an asset purchase, or whether it's a stock purchase. Whatever the transaction structure is, those liabilities don't just go away; they come with the business and the buyer has to deal with them post-closing. And those liabilities can either lead to fines, as you saw in CafePress, or they can give rise to remediation obligations. And I think even more importantly, a buyer could have reputational damage if they buy a company that has poor privacy practices and they don't remediate those practices post-closing and it comes to light. Customers are not going to trust that company anymore.

So, it could affect a buyer's larger operations reputationally if they fail to identify and address these issues. And I think that's why it's so important in M&A that these issues are investigated and dealt with.

Ken Fishkin: Let's talk about some of the key areas that buyers should look at when they're performing their due diligence regarding cyber.

Marita A. Makinen: So, with respect to due diligence on cyber issues, I think one thing it's important to understand is that it's both legal diligence and also operational diligence.

So, the law firm will be asking certain questions. Usually, the client will have someone from their IT group involved also asking questions, or if they don’t have an IT group, if it’s a smaller company, they may hire a consultant to come in and do some of these things. But generally, what we would look at is compliance with laws.

Generally, we would find out: what type of data does the company collect? What business are they in? Again, the most sensitive businesses are around healthcare, financial services, ad tech—any business that's consumer facing and collects a lot of data is going to be higher risk. Does the company know what laws it’s subject to? Do they know where people may be accessing its website from? Do they have a compliance process in place to identify both who is accessing their services and what laws may apply because of that?

We ask what type of policies is the company making public to its customers. Again, we look for those false advertising-type issues that came up in CafePress, and we'd look at whether the company has undertaken audit or third-party testing of its data security to ensure that not only do they have a written policy on record, but they're actually complying with that policy and they're also maintaining physical IT systems that are able to withstand at least a moderate level of attack.

We also take a look at whether a company has third parties that are operating parts of its IT system. We want to know who those third parties are. From an operational perspective, our client will be looking to see are those reputable parties that they feel comfortable dealing with. And from a legal point of view, we'd be looking at what type of contracts are there with those third parties, and do they provide adequate protections?

And we'd also be looking at cyber insurance. We'd want to make sure that the company that our client is buying has cyber insurance that provides coverage generally against costs that may be incurred if there is a data breach. There'll be legal costs; there'll be notification costs; there could be the cost of responding to a government inquiry; or there could be even consumer claims that are brought that have to be defended. Insurance can help cover all of those types of issues, and as a buyer, just like any other type of insurance diligence, we want to make sure that the insurance is in place to cover the major risks that the company is facing.

Ken Fishkin: If you had to pick one thing that would be the biggest red flag for a buyer to back away from a deal regarding cybersecurity, what would it be?

Marita A. Makinen: Well, I guess an obvious red flag is if the company has had known data breaches in the past, the target company in particular. If we think they haven't done proper notifications and that they haven't properly remediated the issue. In that case, this is a case where you could use the escrow approach where the buyer can hold the purchase price back.

Ken Fishkin: Well, thank you, Marita. I'm sure our viewers found this to be very informative.

Thank you very much for watching another episode of Lowenstein Sandler's Cybersecurity video series.