CARLTON FIELDS

Cyber Caremark: Protecting Your Board from Shareholder Derivative Litigation After a Data Loss Event [PODCAST]

September 14, 2015

A company's board of directors has an important oversight role in protecting its company's assets and its shareholders' interests in an environment of increasing cyber threats. Former criminal Assistant U.S. Attorneys and Computer Hacking and Intellectual Property prosecutors John E. Clabby and Joseph W. Swanson discuss key steps that a company should take now to minimize its exposure to cyber litigation in this half-hour *Carlton Fields on Cyber* podcast.

Use the player above or listen on SoundCloud.

TRANSCRIPT Jack: Thank you so much, Christina. I'm so glad that you said, "When a data breach occurs," because that's what's really this is about. There's some things companies could do, in fact quite a lot of things they could do to prevent data breaches, but they're never going to be able to do what it is I think that they want to do, which is 100% protect their companies. So when we meet with our clients, what we often talk about, and Joe will expand on this in the time we have today, but what are their real crown jewels? What are the things that they really want to protect, because that's where they should be putting their assets and their resources. And another thing we talk about is, frankly, how can you protect your company from liability? And in this podcast, what we're going to be talking about is protecting, in particular, board members and senior executives, who in their day-to-day efforts to protect the company's bottom-line, are faced with often-conflicting duties and decisions about how to spend their money. And so Joe, let's get started here. Knowing that these hacks are going to happen, how can a company have any kind of comfort? **Joe:** Well, thanks Jack. And you're right, we can't protect a company from breaches 100%. The news today shows that these events are nearly inevitable. But what's important is to focus on the ways in which companies, the boards, and their executives can reduce their exposure for liability for breaches. And the idea is to make the company and these individuals harder targets for shareholder plaintiffs and for regulators, who are seeking fees, fines, and boardroom trophies. And as we're going to talk about this morning, the aim is to prioritize, make reasonable decisions, and document those decisions, so that if called upon to defend them later there's a demonstrated record of thorough and careful consideration. **Jack:** And this liability really can come from all corners, but I know there are four areas we often talk about as the most likely sources. And we'll start out by talking about the target data breach, and the four corners that these lawsuits come from are these consumers who are angry that their data has been lost, and potentially their identities stolen. Credit card companies and other corporate...we call them contractual counter-parties, things like Amex or MasterCard. And then you also have regulators who are all competing in the public sphere for the attention, and the trophies of taking down corporate executives. And finally - I think something that you and I, I know have written a fair amount about, because of our work with boards of directors - what we call derivative lawsuits, or [shareholders?] who sue CEOs and directors on behalf of the company. So let's talk a bit about Target. If you can maybe give us a quick overview and talk about the litigation. **Joe:** Sure. In Target...and the facts are fairly well-known, but just to provide some context. In the end of 2013, the holiday shopping season, Target experienced a massive data breach, where a third party obtained...rather, stole payment card and other guest information from Target's network. They accessed the network by way of a vendor, and had access to Target's system for a couple of weeks, and during that period of time stole payment card data for approximately 40 million credit and debit card accounts, and in addition, that intruder stole guest information for another 70 million individuals. So it was a massive breach, and the fallout continues. **Jack:** And this was around the holiday time, as well. So for retail companies like this, that's the perfect storm scenario, unfortunately. **Joe:** That's right. **Jack:** So what was the fallout from this litigation in terms of...well,

what sort of litigation was filed against the company? **Joe:** There's been all kinds of litigation filed against the company. Briefly, there were dozens of actions filed around the country on behalf of customer's banks that had issued credit cards and the like. As a general matter, those actions were all moved to Minnesota, where Target is headquartered, and in March of this year Target entered into a settlement agreement that aims to resolve and dismiss the actions filed on behalf of a class of customers whose information was compromised in the breach, and as part of that settlement Target will pay $10 million to the class, as well as attorney's fees and expenses. There was other litigation that involved the payment card companies that issued the credit cards, that had to cover disputed charges and re-issue new cards. That litigation was also sent to Minnesota. And then there was derivative litigation for actions filed against Target's directors and certain of its officers. Those actions were all consolidated in federal court in Minnesota, and those allegations are generally based on the defendants allegedly not preventing or detecting the breach, and failing to adequately disclose and otherwise respond to the breach. And a special litigation committee has been formed in that case, to evaluate the allegations, conduct an investigation, which we'll talk about here in a moment, and ultimately report back to the court. **Jack:** What I appreciate you about that, Joe, is that you've been able to mention the state of Minnesota twice, and I know that's where you're from. And we're as appreciative of you giving Minnesota a shout out-on these conversations we have. **Joe:** Anything I can do. **Jack:** So the $10 million that's going out to the class members, that's dwarfed by one other number that has always surprised me. It's a recent disclosure from the company, but it was a $67 million settlement, not to any class of consumers, but to Visa card issuers. Traditional contract between Target and the Visa card issuers that settled at $67 million. So as much as we talk about where cyber law is going, most of the large scale recoveries, in terms of solid dollar figures against these companies that have experienced data loss, are founded upon fundamental contract principles that are no different than what literally the founders of America were litigating about, when John Adams was a lawyer. So $67 million in August 2015 is a really important number, I think, for executives to remember, that you can do everything they want to protect their companies, but one great place to spend finite resources is on a review of your contracts with third parties and vendors, particularly those who you rely upon for payment systems. Now, in addition to their hard money payouts to the Visa card issuers and to the class members, there have been a couple of other expenditures too. I think Target's latest disclosure talked about $264 million of cumulative expenses for this breach. Now that's been offset by insurance recoveries, but those are only $90 million, right Joe? **Joe:** That's correct. **Jack:** And I think that resulted in net expenses of $174 million, things that were not and could not be planned for. So that's essentially a loss to the company. And it's not over yet. **Joe:** That's exactly right. The special litigation committee that I mentioned that was formed to evaluate the derivative litigation has recently reported that they've met 75 times, have reviewed, and are continuing to review thousands of documents, have conducted approximately 60 interviews, with more interviews scheduled for directors and the officers, all illustrating how costly this litigation, and in particular, derivative litigation can be, just to investigate and get to the bottom line. **Jack:** Joe, can you just say a quick word about what a special litigation committee is? **Joe:** A special litigation committee is often formed once a board receives a demand, either in the form of a letter or some

other communication from a punitive plaintiff, or even after the lawsuit has been filed, which is what happened in Target's case. And that committee is comprised of some subset of the board. They retain counsel to advise them on their work, and they conduct an investigation, and ultimately will either make a binding determination or a recommendation as to what ought to be done with that derivative litigation. **Jack:** So it sounds as if they haven't reached their conclusion yet. **Joe:** That's correct. It's ongoing. **Jack:** And what about regulatory actions? Is there anything happening on that front at least, maybe with respect to the SEC? **Joe:** Well, at least with respect to Target, Target just announced this month that the SEC's enforcement division has concluded its investigation related to the breach, and the enforcement division does not intend to recommend an enforcement action against the company. However, Target continues to have a Federal Trade Commission investigation and other investigations ongoing, from various state attorneys general. And so they're not out of the woods, from a regulatory perspective. One point I'd just like to make about the SEC, they are making a real push to be a player in cyber security. They have issued guidance in 2011 as to disclosure, obligations for public companies vis-à-vis cyber security. Right now, that's merely guidance, but the conventional wisdom is that they're going to be promulgating some sort of rule in that area. The SEC may also, if it does launch an enforcement action in one of these cases, ground that action on some sort of problem with internal controls. The point being that the SEC is working out what their theory is going to be, to justify their involvement in this space. But make no mistake, they are very interested in being a player here, and one needs to do nothing more than read speeches by the SEC chair and the other commissioners about how serious they're taking this issue. **Jack:** I like to think of the SEC as a rancher who's looking out over a canyon somewhere out west, maybe in the 19th century, who's thinking about how they're going to get to the other side of that canyon, and they're shooting arrows across it, shooting guns across it, but one of these days, they may go through the rule-making process, which is the equivalent of building a railroad bridge over that old canyon. I think that's what...you see there's a desire, there is a stated purpose for this, and they're doing everything they can to find a way through, and they'll do it by hook or by crook. So disclosures around cyber security for publicly traded companies, at least, are one area where we know the SEC has authority, jurisdiction, and interest, and that's something we watch pretty carefully. But back to these private shareholder suits. We've talked about derivative lawsuits. I think a word is important on what we've been calling stock drop suits. Now those aren't derivative. Those are not on behalf of the company. Those are on behalf of a class of shareholders who say, "Okay, the stock went down when the news of the data breach hit. How do we recover on this?" Those have had little success, although they are quite costly to the company. And while those are cases we work on, there has not been enough of a development in the law, I think, to know where those are really going. Whereas the derivative cases are starting, and I think we're going to predict a larger push for those, and it's something that really goes to whether the board has invested sufficient time and attention to the company's cyber security. If a company is doing things they need to be doing to comply with their fiduciary duties, if the board is meeting those duties, it's going to be a lot more likely to withstand stock drop suits, derivative lawsuits, regulatory actions, and anything else that comes their way. And these aren't particularly arduous things they have to do. Now let's back up, and let's talk about these fiduciary

duties, Joe. **Joe:** So in the data breach context, one derivative claim that is likely to gain prominence in that you do see in the handful of derivative actions that have been filed related to these incidents, are the so-called Caremark claims, which are premised on a lack of oversight. And Caremark is the name of the Delaware case that defined the contours of this cause of action. The Delaware courts have subsequently said that a Caremark claim falls within the duties of loyalty and good faith, and that's a significant point, because while companies, at least Delaware companies, may insulate their directors from monetary damages for breaches of the duty of care, they cannot do so for breaches of the duty of loyalty and good faith. So a Caremark claim, such as it is, poses real exposure for individuals if there is any merit to them, because it's not something that they can be protected from by the company. **Jack:** So they're out in the open. **Joe:** That's correct. **Jack:** If the plaintiff can meet that standard, the directors are sort of on their own. **Joe:** That's right, subject to whatever insurance they may have, and then some other considerations that we're not going to talk about here. But directors and officers should take some comfort that the standard for a Caremark claim is quite high. A plaintiff has to show the defendants "utterly failed" - that's the key phrase - to implement a reporting system or controls, or if they had such a system in place, the defendants consciously failed to monitor or oversee the operations of such a system. Basically, did they abdicate their responsibilities? Did they ignore red flags? Those are the kinds of things that are talked about with Caremark claims. And while it is an exacting standard, it certainly hasn't prevented plaintiffs thus far, and we think in the future, from asserting these claims against directors and officers, and pursuing them. **Jack:** Now this looks to me like...and in our experience, we've seen, it's an inward-looking lawsuit against these corporate directors. It examines what the board directors saw, who they met with, how long they considered things, how frequently they met to talk about these topics. And that's true, whether you're talking about cyber security, or whether you're talking about executive compensation, or some other board action. It contrasts quite a bit with what the legal process covered, in terms of consumer class actions, which look more like product failure cases. And in that instance you have the class of Target consumers, rather than a shareholder bringing the action, and having to recover based on specific harm to them. Now each year our law firm, Carlton Fields, does a survey of a number of our clients and other participants in the industry on class actions, and the results of this year were pretty stark. That corporate counsel at the companies who participated in our survey saw data privacy failures and particular class actions from consumers for data privacy failures, as one of the paramount worries, the things that keep them up at night. And in some ways, these derivative lawsuits are easier to bring against public companies than the consumer class actions that everyone is afraid of. Joe, why is that? **Joe:** That's exactly right, Jack. One of the reasons why the derivative suit, at least as a theoretical matter and we think, in the future, as a practical matter, that you're going to see more of them, is that there's no problem of alleging and ultimately proving a class-wide loss, and that's because of the derivative action. All it takes is a single shareholder to bring a derivative action that's founded on an alleged harm suffered by the company. And that harm could be alleged to be the result of the expense of containment, legal fees spent on the data breach, costs associated with notifying affected consumers, damage in the form of regulatory actions, and just a diminished reputation among the public and consumers. All of those

costs could be alleged by a derivative plaintiff as having harmed the company, and giving rise to a derivative claim. **Jack:** And that's a good point, too. And when you think about how this contrasts in the investment that either the shareholder or the shareholder's lawyer has to make. Consumer class action is a significant complaint to bring, it requires quite a bit of work and research to have it be brought, and to get past the motion to dismiss. The initial investment that a shareholder or their lawyer has to make for a derivative lawsuit is a letter. It's a letter that they write to the board, demanding that the board take action against the executives. And as a result of this an entire process, a huge expensive process gets initiated by the company to defend itself. And this letter can really just parrot the company's press release regarding the breach, you can look at what the regulator may have announced about it, or it can follow piggy back on either a consumer class action that's already been filed, or shareholder stock drop class action. **Joe:** That's exactly right. And because it can be so expensive to investigate and respond to a shareholder demand for a derivative action, as well as the cost of defending the litigation on the merits, oftentimes the corporate counsel's calculus as to one of these suits is going to point to an early settlement, so as to avoid that expense and nip it in the bud, so to speak. And frankly, that's no secret to the plaintiff's bar and is another reason why we expect these types of actions to put proliferate. **Jack:** That's right. And unlike some of the consumer class actions that have been discussed for the past few years, most states' laws that govern derivative actions provide for attorney's fees, for the shareholder who successfully has either a favorable settlement or a court win in these derivative lawsuits. So there's a prize at the end of this, where that work is rewarded. And that may be something that shareholder counsel who are out here looking for ways to break into the cyber marketplace are valuing cases. Now all these contrasts should make a board of director a little bit nervous. Are they doomed? **Joe:** No, they're not doomed. And what we're going to talk about now are the things that the board and the senior executives can put in place so as to mitigate their exposure. And the keyword here is 'process.' There needs to be a process in place, so that the board and the senior executives stay informed about the company's cyber security. These individuals need not dwell on the outcome. Again, it is virtually impossible to make a company cyber-proof, such that they're never going to experience a data breach. But rather, with that reality in mind, they need to work back from that, and design a process that keeps them informed, permits them to make reasonable decisions that can be defended later on, when challenged. **Jack:** So if you're a company that says, "Okay, I'm on board with this. I want to make sure that our directors are doing the right thing," where do they get started? **Joe:** Well, the first thing they should do is conduct a risk assessment that really focuses on the company and the types of data that the company holds. So understanding the company and its data, identifying that data, and grouping it in buckets, and then assessing the likelihood of each of those buckets of data being accessed or compromised by an outsider, and then evaluating what the impact would be on the company if any one of those, if not more, of those buckets were accessed or compromised. It comes back to what you said at the beginning of our discussion, Jack, which was identifying the crown jewels and prioritizing, because people are dealing with finite resources and they need to make difficult decisions, and to do that they need to understand what their data is, and where the risk is. **Jack:** And that's right. And this risk assessment becomes the north star as we navigate the rest of

these steps. The risk assessment, as companies acquire business units, as they shed business units, the risk assessment as to which of these buckets we're most concerned is going to change, and when it changes, everything that follows it has to move. Now this is no surprise to post Sarbanes-Oxley world. This is a no-surprise to companies that have enterprise risk management. What we're proposing is that cyber simply become part of that enterprise risk management, and when the word 'cyber' gets mentioned at your board meetings, your pulse shouldn't go up. You have a process in place. Your risks are dealt with. You're not talking about protecting against a meteor strike. You're talking about what's likely to happen, based on the data you have. And once you do this risk assessment, how do you start operationalizing it? Well, then you draft policies and procedures about how to handle this data. We have the crown jewels in the Tower of London, we need to put a guard up around it. We don't need to put a guard in Paris, we need to put a guard in London near where the crown jewels are. **Joe:** Right. **Jack:** And once those policies and procedures are in place, a compliance team now can test against them. Outside auditors can audit them. People can start doing their job that they normally do with any number of these risks. So step one, risk assessment. Step two, draft your policies and procedures, then test them and audit them. Where do they go from here? **Joe:** Next, the board and the senior executives ought to consider whether they need some sort of outside help, and they ought to undertake that evaluation in connection with drafting an incident response plan, that is going to be tailored to the company's regulatory and legal environment, and its business risks, and frankly just the nature of its business. Where does it do business? Where are its customers? Who is its principle regulator? What are their expectations vis-à-vis cyber security? You need to know all of these things and they need to be documented in an incident response plan, so that when the inevitable happens, you know who you need to call, when you need to make that call, who you need to notify, and so on and so forth. And that incident response plan can include the thresholds that ought to be in place for when the board needs to be notified and brought in when a data breach occurs, or some other cyber incident. And I don't think the board needs to be notified in every instance, but rather, I think it's fair to say as a general matter, from medium to serious breaches the board ought to be brought in, made aware of the situation, and those thresholds should be memorialized in your incident response plan. And that plan can be drafted, again as I mentioned, with outside help, whether it's outside consultants, outside counsel, all of them are willing to help get this plan in place. **Jack:** Right. Your plan needs to include as granular items as you can put in there, and may include the name of the person at the cyber response team who you're working with as your third party vendor. Put the name and the phone number of the lawyer who you've already talked to, who helped to put this together. Have it on there. If you use an outside media consultant, put their name, put their number on there. And all these documents now that you've created: your risk assessment, your plans and procedures, now your incident response plan, you don't put them in your closet. What companies need to do is train their staff. And you train your staff appropriate to their level of responsibility, and you train your staff appropriate to their role in the incident response plan. The important thing for the board is that the board receive updates on this training being done. So the board will then, at this stage, be aware of these written documents, the policies and procedures and the incident response plan, and will learn that the staff has been appropriately trained on them.

And I think one other part that's pretty important at this stage to mention is that risk management, or the general counsel's office, or whoever in a company has responsibility over insurance policies needs to take a pretty careful look at them again. Talk with your broker about these things. Consider obtaining cyber insurance to address this exposure. The principle rule of insurance is to insure against catastrophic risk. Some... depending on your company, a loss or a data breach can be that sort of catastrophic risk, and it's exactly something you need to review for your insurance coverage. Now what else, if anything, does the board need to do or the board need to see gets created, in addition to these writings, Joe? **Joe:** As a general matter, and just as an aside, this next bit of advice also should be tailored to the company and the board and its composition. If the board has members who are well-versed in these issues and technology generally, this next bit of advice may be less important, or perhaps these are the people who should be tasked with the things we're going to talk about. But as a general matter, there should be a board committee, or perhaps an existing board committee, perhaps the audit committee or technology committee, who is charged with focusing on data protection issues, and for lack of a better term, that could be the cyber committee. And there should also be a lead board member for data privacy issues, the lead cyber director, so to speak. That the board can look to this committee and/or this director for guidance on these issues in addition to looking to counsel, but again, it should be some person or group of people who have some experience. And if no such people exist on the board, then outside consultants can be brought in as well, to provide that expertise. There also should be within the company a chief information security officer, or equivalent position, who has reporting duties to the CEO, or directly to this cyber committee on the board. In either event, what you want is there to be an open line of communication for frank, unfiltered contact between the board and this chief information security officer, so that all the important information is communicated to those who need to know it, when they need to know it. **Jack:** All right, so now that your company has a policy, now that your company has a response plan to a data breach, and the right people are in place to oversee and receive updates on this, this process needs to put in place a continual or periodic updating itself. And these updates when they're done, it's re-calibrating where the north star is, right? What we talked about at the beginning of this piece is you have to know where your risks are, and those risks change. These can't be locked in stone. This isn't the Magna Carta, this is something that's more like an operating agreement that changes from time to time, and is amended in real-time. The cyber committee or whichever committee of your board of directors has received this sort of designation, should meet at least quarterly on any major changes to the risk assessment itself, to the policies and procedures, and to the incident response plan. If there are other changes outside those three major buckets, that can probably be done annually, and frankly it can be done even at the board level, rather than at the more specific level, because the board, in addition to the special committee, should get at least annual updates on the state of cyber security. And all of these things, all of these efforts from the initial risk assessment through to the updating of the plans and the updating of the board need to be memorialized. And from the case law that we've looked at, we can't emphasize this aspect of it enough. It's important to do these things to protect your company. It's important to do these things to protect the directors from liability. But if you don't have a record that it was done, and if that

record isn't kept in a place, when bad things begin to happen, when breaches begin to happen, and when lawsuits follow the breach, you're making your life a lot more complicated. You're raising the cost of your compliance effort, and you're hurting yourself if you don't have them organized in one place. **Joe:** And Jack, in that regard, isn't it no different than what we all learned in middle school algebra, to show your work? **Jack:** That's exactly right. It's...you got the answer right? Hey that's great. You had enough meetings. But if your meeting minutes don't reflect it, if they don't reflect that there was a give-and-take, if it doesn't reflect that the chief security officer made that briefing, you're not going to be able to knock out that lawsuit early on. Even if you've done all the right things, if you haven't documented them, you're dragging yourself out into a much worse fight. **Joe:** So it sounds like you need to have those meeting minutes handy, and in a centralized location, so that they can be pulled off the shelf if the company does suffer a breach and there's some sort of regulatory action or litigation. But just stepping back, when the breach occurs, what are the handful of things that the company needs to do to spring into action? **Jack:** That's right. And the company who's followed this advice, the general plan to have their writings in place and the people in place, the first thing you do is you activate your incident response plan. it's much like...to go back to the example from school days, it's a fire drill. We've drilled for this, we have procedures for this. Like in an elementary school classroom, there is a map that shows you exactly where to go. Go there, do that. Trust your training. Do the things that you say you want to do, and if that...that incident response plan should also have some calibration to the size of this. If it's something that is small and you've activated your incident response plan, brief the lead cyber director. It doesn't need to go to the whole board. But if it's something that's significant, if senior management and executives are working hard on it, then that board needs to know, and they need to know pretty quickly. Now, during this briefing when it happens for major incidents, management needs to provide the directors with not everything, but just the key information and it should be documented that that process has taken place. The minutes need to be accurate. They need to reflect the level of information that was shared with the board. And I think frankly, it needs to show a question and answer period. If there are third parties who are working with the board, who are working with the company to help them contain the breach, they should be made available to the board, so the board can ask unfiltered questions. If these steps had been taken right, the board has a trust relationship with each chief information security officer, and will gain comfort that its questions are being answered truthfully, and that the company is being steered toward that north star that we talked about at the beginning of this. So in summary, I think for that it's you activate your incident response plan. For major incidents, report it to the board. For minor incidents, report it in the ordinary course. During this briefing, management needs to provide the directors with just the key information, but these briefings happen often, that they happen early, and that they happen with an open dialog. Minutes of these meetings need to be kept carefully, and after the breach has been contained, everybody needs to get back together, talk about lessons learned, then they need to go back to that north star determination and see, "What can we do differently next time?" **Joe:** The good news, Jack, as we wrap it up here is that the same corporate governance practices that should insulate or at least minimize exposure for directors and officers from derivative liability, should also protect them and their companies from exposure to regulators.

Again, they and their counsel need to focus on process over perfection, and recognize that these incidents, cyber incidents, are inevitable for most companies. And that courts and regulators are likely to understand that and be sympathetic, and look more favorably on directors and officers, who prior to the incident befalling the company had in place processes that were documented and that were designed to assess risk, deploy resources appropriately, detect the breaches, and respond to any incidents in a meaningful, timely way. **Jack:** And if you're doing this, you're not only protecting your shareholders, but you're protecting consumers, and you're protecting your board and your management. All the things that are going to keep you out of trouble down the road. Well, that's our time for today. Thanks to everyone for tuning in. I'm Jack Clabby. **Joe:** And I'm Joe Swanson, and this has been Carlton Fields On Cyber. Thank you.

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Securities Litigation and Enforcement