Fox Rothschild Podcast

Featuring Partner John Gotaskie

We are talking today on FoxCast with John Gotaskie about data hacks and the tough lessons that organizations need to learn. John is a partner and litigator with Fox Rothschild in Pittsburgh. He represents individuals, partnerships and companies in diverse legal matters including complex commercial litigation, bankruptcy litigation and franchising issues. John also is editor of the firm's Franchise Law Update blog. John, good morning.

John Gotaskie: Great to be here.

***Question**: John, you recently wrote a post for Fox Rothschild's Franchise Law Update blog that got a lot of play – you titled it "What To Learn From the DNC Hacks."*

John Gotaskie: I did. The data breaches experienced by the Democratic National Committee, as well as others including former secretary of state Colin Powell and the World Anti-Doping Agency, have been hot topics. The headlines from those events over the last two months from both the business world and presidential campaigns and the Olympics remind us that our data security is constantly under attack. Whatever you think of the campaigns this year, you really do need to resign yourself to the fact it's not just them – you are almost certainly going to be hacked as well.

***Question**: John, aren't there firewalls and other traditional protections? Aren't they enough?*

John Gotaskie: No. I'm not suggesting you should forget about electronic walls or moats or fences or whatever analogy you want to use. You'd be foolish in fact not to have them. But the number one thing to remember is this: 100 percent deterrence is practically impossible to come by, unless you want to unplug yourself from the internet entirely. And we all know that's not realistic in today's world.

***Question**: John, you're then advocating that franchisors focus on containment rather than prevention.*

John Gotaskie: Absolutely. Because I think again they are timely, I'd like to offer a couple of observations I made about the alternative strategy of containment several months ago.

***Question**: John, what's the first?*

John Gotaskie: The first is the most important. Acknowledge that, while necessary, those security walls or moats and other deterrence measures are highly unlikely to be 100 percent effective at defeating determined hackers.

***Question**: Hmmm. What else?*

John Gotaskie: After you acknowledge that first step, you first have to admit to yourself that breaches of your data are going to occur.

***Question**: So, as you're saying, if the inevitable breaches occur, then what to do? What do you recommend?*

John Gotaskie: You have two plans in place: one for *before* the hack and then one that you put into place *after* the hack has occurred.

***Question**: Tell us more.*

John Gotaskie: The "before" plan has to include a detailed review of what data is stored on your systems and where is it stored. This is absolutely essential. You've got to map it out so you know what you have. And take a hard look. Find out if you've discovered that you really need all of the data being stored. You might discover that as storage has become cheaper, more and more data is being stored for longer and longer periods of time, whether you intended to or not. So conduct a review with all of your vendors as well. In many of the high profile cases of breach over the last three years, it wasn't the franchisors' systems that were hacked. It was the vendors' systems were hacked and then they used the vendors' system as a "back door" into the primary target. Similarly, just like vendors, a lot of issues have come up in the franchise world involve what your franchises are doing with data and what kind of protections they have. You've got to establish and share suggested best practices that can guide your franchisees and your vendors on all of these issues.

***Question**: So, John, that's the "before" part. What then about the "after?"*

John Gotaskie: The "after" is the plan you have in place to put in after you've been hacked, right? So you've got to have your people in IT, your insurance people, your public relations people, your marketing people, your social media team, your legal team, all of them in place ahead of time and a response plan ready to go. Granted, it's going to have to be flexible. You're not going to be able to predict exactly what happens. But the most important thing is that having it in place ahead of time, you're going to be able to get in front of the breach. You want to be able to reassure your customers and if a franchisor, your franchisees, that you are putting their interests first, that their information is protected. This includes being ready to lend a helping hand to franchisees suffering breaches. Remember, your brand is on the door. That's the name that will lead all of the news reports about the hack. Now is the time to develop your plans. Customer loyalty at the end of the day will depend upon your preparation.

***Narrator**: Well, thank you John. Listeners, to confidentially discuss your organization's approach to data protection, please contact John Gotaskie in Pittsburgh at 412.394.5528 or at jgotaskie – that's J-G-O-T-A-S-K-I-E – at foxrothschild.com.*

Fox Rothschild LLP is a national law firm with 750 attorneys practicing in 22 offices coast to coast. Our clients come to us because we understand their issues, their priorities and the way they think. We help clients manage risk, and make better decisions by offering practical advice. Visit us on the web at www.foxrothschild.com.

# # # #