F P L G
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Blackbaud Data Breach: Fallout for Nonprofits

09.29.20 | Linda J. Rosenthal, JD

There have been cyber attacks for as long as there's been an internet.

Experts have long run around with their hair on fire to warn all of us about the serious dangers lurking in the shadows by hackers and fraudsters. As we now know well, cyber attack victims are not only huge, for-profit businesses and wealthy individuals. Nonprofit organizations, large and small, are the targets. "Hackers do not care what you do, only whether you have records they can harvest" we explained in our first post on this important topic, *Nonprofits And Cybersecurity: Make It A Priority* (November 30, 2016). "It's a factor for any organization with digital record-keeping."

Now, at the end of September 2020, we're trying to make sense of the breadth and scope of the massive hack of South Carolina-based, Blackbaud. This firm is one of the world's largest providers of financial and fundraising technology to nonprofits.

This is a still-unfolding story, although the "pfishing" breaches occurred many months ago between February and May. And that, of course, is a big part of the problem. There was a delay in discovery by the direct victim, Blackbaud. There has been controversy about how the aftermath was handled, including significant delays in that firm's reporting the breaches to the first level of indirect victims, the nonprofit clients. The extent to which the ultimate victims – donors, beneficiaries, service recipients, and others whose data was stolen – have been notified at all or sufficiently remains unclear.

And now there are lawsuits.

Blackbaud's Data-Breach Missteps

One of the most common types of computer intrusion is "phishing." That term was "coined around 1996 by hackers stealing America Online accounts and passwords. By analogy with the sport of angling, these Internet scammers were using e-mail lures, setting out hooks to 'fish' for passwords and financial data from the 'sea' of Internet users."

A few years ago, cyber security expert, Lisa Traina, CPA, explained that "…[w]hile cyber breaches can take many different forms, they typically occur when hackers target three common weaknesses :…phishing, vulnerabilities, and malware." These are the "… most common threats for nonprofits."

The Blackbaud situation has been described as a series of classic "pfishing" maneuvers, reaching into data supplied by nonprofits from around the United States and the United Kingdom and elsewhere. The cyber criminals followed up the May 2020 discovery of the hacks with the usual coup de grace: a "ransom" demand for return of the stolen data. Aided by law enforcement and outside security consultants, Blackbaud says it negotiated and paid the "ransom" about a week later after – according to the firm – it received assurances that the stolen data was returned without any compromise.

But it wasn't until mid-July 2020, that Blackbaud first reported it publicly and began to notify its clients. See, for instance, *Breaking: Blackbaud Hacked, Ransom Paid* (July 16, 2020) Paul Clolery, *The NonProfit Times; Blackbaud Pays Ransom Demand but How Much Damage is Done? (July 24, 2020) Ruth McCambridge, The Nonprofit Quarterly; Fall-Out from Blackbaud Ransomware Attack* (July 24, 2020) Linn Freedman, Esq., Robinson+Cole; *Questions Persist About Ransomware Attack on Blackbaud* (July 30, 2020) Mathew J. Schwartz, healthcareinfosecurity.com.

Since then, the facts have continued to dribble out, slowly and incompletely. And that's why now – two months later – Blackbaud is being hit with class-action lawsuits. Many nonprofits – large and small – are left wondering what they need to do next. See, for example: *The Hack Of Blackbaud: Damage Is Still Being Assessed* (August 6, 2020) Paul Clolery, *The NonProfit Times; Blackbaud Ransomware Breach Victims, Lawsuits Pile Up* (September 24, 2020) Marianne Kolbasuk McGee, HealthInfoSec; *Lawsuits Proliferate in Blackbaud Incident: Nonprofits, Consult Your Lawyers* (September 25, 2020) Ruth McCambridge, *The Nonprofit Quarterly.*

Blackbaud's Nonprofit Clients in the Middle

Because of the pervasiveness of the threat of cyber attacks, and the catastrophic amount of damage that invariably follows a computer breach, cyber security should be near the top of the list of planning and risk-management concerns for nonprofit board members and senior staff.

But many organizations fall well short of that goal. What's the key obstacle – (then and now) – to nonprofit organizations taking adequate precautions? First, it's "… the highly technical, complex nature of this 21st-century crime. Nonprofit organizations are unequal in their ability to have or obtain sufficient expertise to handle this complex matter.

Second, it's the long list of other priorities made worse this year, of course, by COVID-19 challenges and disruptions.

Third, there are complicated reporting duties, both moral and legal, enhanced by relatively new laws including the General Data Protection Regulation and the California Consumer Privacy Act. In addition, nonprofit health care entities have additional legal requirements under the federal Health Information Portability and Accountability Act (HIPAA).

For nonprofit clients of Blackbaud, there is also an extra layer of complexity because they are in the *middle* between the direct hacking victim – Blackbaud – and the indirect victims of the stolen data. There are "… multitudes of not-for-profits [that] have received notification of the incident [but] are struggling with how to respond. The responses have been anything but uniform."

Of course, the "delays of several months have made the position of the nonprofit client that much more precarious."

Conclusion

As the full facts and circumstances of this news story unfold in the coming weeks, we'll revisit this topic to discuss questions and issues that are of interest to the nonprofit sector. [Update 9/29/20]: *Breaking: Some Donor Data Accessed in Blackbaud Hack* (September 29, 2020) Paul Clolery, *The Nonprofit Times.*

— Linda J. Rosenthal, J.D., FPLG Information & Research Director