Report on Patient Privacy Volume 20, Number 12. December 10, 2020 In Part 2 of Q&A, Data Breaches Blogger Discusses Why Ignoring Her Is a Bad Idea

By Theresa Defino

Among a trio of recent settlements the HHS Office for Civil Rights (OCR) announced over hacking incidents was one for $1.5 million with Athens Orthopedic Clinic PA, which involved an intrusion by The Dark Overlord and an unusual tip provided by "Dissent," a pseudonymous blogger for Databreaches.net—a must-read for HIPAA privacy and security compliance officials.[1] In part one of a wide-ranging Q&A with *RPP* that ran in the November issue, Dissent, a retired psychologist from New York who does some breach-related consulting work, discussed why she doesn't use her name, her views on the settlement and the psychology of hackers.[2]

In the conclusion to the Q&A presented here, Dissent described the reactions of some she tried to notify of a breach, how *not* to react and what she finds frustrating—and satisfying—about her efforts. She also shared the one thing she thinks most organizations are lacking.

***RPP:* OCR credited you with notifying Athens of its breach. What is your goal when you contact a company?**

D: The first goal is to make sure the entity knows that they have a problem so they can lock down their files and start incident response. I don't want to report on anything while it's open. I'll tell them what I have seen or learned. I may give them a URL to find their leak, or I may include a snippet of data as proof.

Like with Athens Orthopedic and other breaches involving The Dark Overlord, they weren't announcing who their hacking victims were. I figured out who they were on the first day, and I named them in the blog after contacting them. I had some of the other victims ignoring me or yelling at me because I don't think they wanted me knowing. And they would try to say nothing was going on, but I knew it was. I had the proof.

***RPP*: When you suspect, or confirm, a breach, do you immediately notify the organization?**

D: It depends on how I'm getting possession of the information. If a researcher contacts me with it, I'll say, "Have you contacted them? Have you notified the entity?" I've worked with researchers to get them to do more notifications themselves. And I've had them set up accounts that they can use to protect their identity, because a lot of these guys are scared that they're going to be accused of hacking, and wondering if they downloaded the data, will they be in trouble with the law. You will see in my reports I don't always identify the researchers. If they don't notify, then I notify.