The Federal Lawyer in Cyberia

by Mike Tonsing

Merchants Are Mining Facebook, and I Guess I Am OK with That—Sort Of.

Last week, I received one of those delightful "wake-up call" form letters that come from large banks and corporations all too frequently now, letting me know that I may be among the millions whose credit card information and other private data may have been compromised as a result of the sender's database having been hacked.

Lovely! Here we go again. The form letter suggested that I should be vigilant in examining my credit card statements. (That is as valuable a tip as the one I love from software help desks—I should ensure that my device (the one I have just told them has all of its lights flashing) is plugged in.) I suppose I shouldn't be angry, but I am.

Perhaps, after all, it is better that some hacker has my credit card information and my mother's maiden name than that opposing counsel has my privileged e-mails to my client.

But, whatever the case, I've been reminded once again of the fragility of Internet security and of my own privacy. Over and over again, for as long as reality allows me to each time, I delude myself into thinking I am secure because I have five-star-rated antivirus software installed and because I have a highly recommended firewall in place, but eventually—each time—reality intrudes and I must again face the fact that if the large banks and corporations can be hacked, and if the highly sensitive computers operated by federal agencies can be hacked, and if the Defense Department's most sensitive systems can be hacked, so can my credit card, despite its puny $5,000 or $10,000 credit limit that is probably not very important to anyone but me—and some anonymous guy in an unpronounceable third-world country who uses it to buy books from Amazon and exploit my credit rating. But, not to fear. (There I go again!)

Turns out, the problem is a lot bigger than that. According to a well-regarded outfit known as Cybersource Corporation, the scope of online fraud is a whole lot larger than I had previously allowed myself to believe. It is a lot more than just an annoyance and a dutiful form letter. Because of its size, someone may eventually heroically arrive on the scene to protect me and you. Maybe they're already here. But first, let me put the problem into perspective.

Cybersource, a wholly owned subsidiary of Visa, Inc., has a nearly global reach. It is, of course, also very well respected in the industry. It reports that financial fraud on the Internet resulted in losses totaling roughly $3.5 billion in North America alone in 2012. Yes, that's right, three and a half billion dollars. (To gain some perspective, e-commerce spending in the United States is expected to hit $262 billion this year, according to Forrester Research.) And, mobile e-commerce growth is huge. According to comScore.com, sales transacted via cell phones and tablets are expected to surpass $25 billion, or one out of every $10 spent online, by the end of 2013.

Cybersource has indicated that the per-order value of fraudulent transactions perpetrated here in the United States tends to be, on the average, about $200—about one-third higher than the average value of a valid order, $149. Crooks are getting bold, and they are casting their Internet nets widely. These Cyberian crooks are not confining their fraudulent activities to the United States. Cybersource calculates that currently 2.9 percent of online orders are rejected due to a suspicion of fraud in the United States or Canada while outside of those two countries (i.e., in the rest of the world) the average percentage of orders rejected due to suspicion of fraud is 7.5 percent.

There's an old expression—fight fire with fire. Imagine using data available on the Internet to combat the fraudulent use of Internet data! A Palo Alto-based startup that launched out of beta status last October is doing just that.

Signifyd Incorporated has a website that proudly proclaims, "No one combines data sources like us." This company, formed in 2011, has recently announced a software-as-a-service product that analyzes 120 data points *that include a customer or applicant's social media posts* to deduce whether a pending credit transaction is likely to be fraudulent. "We make fraud review simple," proclaims the Signifyd website, www.signifyd.com.

Signifyd is not the "first to market" as an online fraud protection company for creditors. Others have already occupied the same space. (They include MaxMind, Kount, ThreatMetrix, and Accertify.) However, Sygnifyd boasts that it is the first company to market with a product that instantly plumbs the social media clues provided by credit applicants.

Rajesh Ramanand, co-founder and the CEO of Signifyd, was recently quoted in the *Silicon Valley Business Journal* as stating that by analyzing a user's online and offline footprint—including their social media postings—the software can instantly and intelligently tell an

---

Michael J. Tonsing practices law in San Francisco. He is a member of the FBA editorial board and has served on the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California. See www.TonsingLawfirm.com. He also mentors less-experienced litigators by serving as a "second chair" to their trials (www.YourSecondChair.com). He can be reached at Mike@TonsingLawfirm.com.