# Cooley

August 11, 2014

As you have probably seen, it was announced on Tuesday, August 5th, that usernames and passwords from 1.2 billion Internet accounts from over 420,000 websites were stolen by a criminal organization in Russia. According to additional information we've received and other press reports, a Russian cyber gang known as CyberVor acquired databases of stolen information that were used to engage in phishing attacks. They then moved on to using botnets that exploited websites with SQL injection vulnerabilities.

While the names of the compromised websites have not been released, we recommend that you assess whether your organization may have been affected and, if so, what action needs to be taken. FIRST, talk to your IT department about whether there has been any unusual activity on your network. SECOND, find out from your customer service department whether any complaints or concerns have been raised by customers. THIRD, for companies that have not performed a security audit recently, this might be the time to do so. FINALLY, if you find that you are the victim of a security breach, our Privacy & Data Protection practice group (PDP) can help you.

From a customer-facing perspective, we further recommend that you provide advice to your customers that may help them with not only your particular site but also with other sites they may visit. In particular, customers need to be made aware that they should be vigilant and monitor activity of any websites to which they have registered. If they identify suspicious activity, they should change the password of that site and contact the appropriate support personnel.

We recommend that your customers consider the following when creating passwords so as to minimize their exposure to hackers:

- **Do not use the same password**. When hackers get username and password information for one site, they begin to try them on other sites. If you use the same password for e-mail as you do your bank, a compromise of your e-mail provider easily puts your finances at risk if the passwords are the same.
- **Use complex passwords**. Create passwords that are greater than 8 characters and have a number, letter, and special character. A common method is to use a sentence that is easy to remember like "I love C00ley!"
- **Get a password safe**. There are many password safes for your smartphone or home computers so you can easily store all your passwords.
- **If available – use two-factor authentication.** If a site offers additional security features like secondary or two-factor authentication, enable them. Then, when you enter your password, you'll receive a message (usually a text) with a one-time code that you must enter before you can log in. Many bank sites and major sites like Google and Apple offer two-factor authentication. In some cases, the second authentication is required only if you're logging in from a new computer.

Cooley PDP attorneys have substantial experience leading incident response efforts and advising companies (including those in the online, retail, financial services, technology, and life sciences fields) that have experienced data breaches or other data security incidents. For incidents that trigger regulatory investigations or class action litigation, we put together the right team with the appropriate experience to handle all aspects of the client's problem, and we take a collaborative approach to developing solutions in the most strategically sound, practical, and cost-effective manner.

If you do happen to be affected by this latest massive attack, please give us a call. If you have not been a victim, you may nonetheless want to consider a cybersecurity liability "tune up." Using well-known and industry accepted techniques (e.g., the NIST Cybersecurity Framework), we can help you figure out what protections would be most appropriate for your organization. We look forward to speaking with you.

## Key Contacts



| | |
|---|---|
| Michael Rhodes<br>San Francisco | rhodesmg@cooley.com<br>+1 415 693 2181 |
| Matthew D. Brown<br>San Francisco | brownmd@cooley.com<br>+1 415 693 2188 |
| Randy Sabett<br>Washington, DC | rsabett@cooley.com<br>+1 202 728 7090 |