BEBCHICK LAW

Law Alert May 2011

Welcome from Bebchick Law

Dear Clients, Colleagues and Friends,

This Alert is intended to update you about newsworthy legal issues and developments. In light of the recent massive Sony PlayStation Network hack, we outline the obligations of a systems operator who falls victim to a data breach. And we briefly discuss the significance of a recent Supreme Court decision which may enable businesses to insulate themselves from class action lawsuits.

Also included below are links to two articles we recently authored: one about running a remote business (in our case a law practice) which appeared in the *New York Law Journal* and another about start-up issues for entertainment clients (geared specifically to filmmakers):

Remote Practice

Entertainment Start-Up

We hope that you find this Alert instructive, and we look forward to any feedback you might have.

Best regards,

Baruch M. Bebchick

How to React to a Data Breach

The recent major hack of Sony's PlayStation Network, involving the theft of personal information from its 77 million subscribers, has sparked numerous inquiries to us about data breach compliance over the past several days.

The PlayStation Network, which enables online users to view movies and play interactive games with multiple participants, was compromised by hackers on April 17. Sony took the system offline on April 20, the day after it detected the breach, but waited until April 26 to publically disclose that the network had been compromised.

In This Issue

Contact Us:

646 688-4375

Email

Website

Bebchick Law is a vibrant corporate and intellectual property law firm with a focus on business law. Our practice services a broad mix of businesses in various stages of growth.
We regularly counsel clients about how to most effectively organize and reorganize, structure entrepreneurial ventures, and commercially protect and exploit their intellectual property and other assets.

On May 2, Sony further announced that its Online Entertainment platform also had been broken into and taken offline the prior day.

So it has not exactly been a good two weeks for Sony. And there is more to come. While a full picture has yet to be provided of exactly how the two Sony data breaches occurred, various affected subscribers have already responded by filing lawsuits, and numerous regulatory agencies and state attorney general offices have begun to investigate the appropriateness of Sony's reaction to the massive breach.

At first glance, Sony does not seem to have responded particularly well. Its decision to wait six days before making a public disclosure of the breach and the unauthorized access of its users' personal information has been highly criticized. This delay seems especially egregious given that the credit card information of Sony's users was evidently part of the compromised data.

So what can we learn from the PlayStation Network data breach and Sony's response? And what should businesses who own online systems, or even just maintain the personal data of customers obtained over the Internet, do in the unfortunate event of falling victim to a data breach?

The following is a brief list of key items to consider:

1. Determine Applicable Legal Obligations. When faced with a data breach, first consider which laws govern your handling of the situation. There is still no single federal law or regulation which addresses the security of all types of personal information, though federal law does govern certain industries (e.g., health care providers and financial services providers). In the absence of comprehensive federal legislation regarding data breaches, all but four states (Alabama, Maryland, New Mexico and South Dakota) have implemented their own data breach laws. Most of these describe the type of data requiring protection, set forth a time limit and methods by which notice of a breach must be provided, and in some cases require the implementation of information security programs to protect the security, confidentiality, and integrity of user data.

In New York, the statute regulating data security breaches is the New York State Information Security Breach and Notification Act of 2005 (the "Act"). It applies to data breaches involving individuals or entities conducting business in New York that affect state residents. The principal requirement of the Act and similar laws of other states is the prompt provision of notice to affected users.

The Act applies to those data breaches where unauthorized access to "private information" has occurred. "Private Information" under the Act means, in addition to personal information about an individual (e.g., name, email address, etc.), either such individual's (i) social security number, (ii) driver's license number, or (iii) credit or debit card number. Note: since Sony conducts business in New

Business Formation & Reorganization

IP Management & Exploitation

Internet & e-Commerce

Media

Corporate & Commercial

Licensing

Strategic Ventures

Employment

Software

Marketing & Advertising

Entertainment

York, victims of the breach included residents of New York, and credit card numbers were allegedly part of the information stolen, Sony is indeed subject to the Act's provisions.

However, if a data breach of personal information does not include any "private information," then a system operator will not be subject to the Act's provisions. This is most likely to occur if a hacker is unable to access credit card numbers or other encrypted information, but is able to reach other personal information of users. That said, you should keep in mind that several state's data breach laws have a broader reach than the Act's provisions (for instance, other state laws apply to all unencrypted information compromised rather than just to "private information"). So a system operator who becomes the victim of a data breach must consider each applicable state law on a per-case basis in order to determine whether the breach, and the operator's response, is governed by such law's provisions.

2. Minimize Damage with Prompt Notice. If you find yourself subject to the Act or another state data breach law, you must expeditiously comply with all applicable obligations. The most pressing of these in most cases will be the notification requirements. The Act mandates that notice to affected users must be provided in the "most expedient time possible without unreasonable delay", but also provides that notice should be consistent with needs of law enforcement and take into account the scope of the breach and the goal of restoring reasonable integrity to the compromised system. For instance, the Act permits a delay of notice if an investigating law enforcement agency determines that such notification will impede a criminal investigation into the cause of the breach.

3. Think PR. Even if you are under no obligation to comply with the Act (or another state's data breach law), in many cases it will be prudent for you nonetheless to adhere to such notification requirements. This will not only be expected and appreciated by those users whose data has been stolen (by enabling them to take timely remedial action), but in many cases will also take the wind out of the sails of potential lawsuits, gripe sites, and industry specific or consumer-rights blogs. We suggest devoting significant resources, if necessary, to getting out your story early and clearly; an effective response will more than pay for itself in avoided lawsuits, a positive (or at least a not such a negative) media profile, retained customers and overall goodwill. And you should consider using a personal touch by contacting each affected user by email and follow-up telephone calls. Note: the Act requires that you keep logs of electronic and telephonic communication of any such notice, so be sure to comply with this provision.

It also would be wise for you to include in your notice (or in a follow-up communication) additional information helpful to affected users, including suggestions about how to protect against significant consequences resulting from the unauthorized use of their stolen data. To illustrate, you may wish to recommend that users

Trademark & Branding

Outsourcing

Biotech

Privacy

Business Formation & Reorganization

IP Management & Exploitation

Internet & e-Commerce

Media

Corporate & Commercial

Licensing

immediately contact their credit card companies, monitor their credit card billing statements and obtain a copy of their credit report in order to determine whether their credit card information has been misused. You might also suggest that affected users be watchful for phishing scams (since the hackers who compromised your system could be posing as you and contacting users through their stolen email address), and that they change their login IDs and passwords for other accounts (since many people use the same login ID and passwords across many different systems).

4. Protective Provisions. If you become the victim of a data breach, you should engage an independent cyber-security investigative firm to probe the cause of the breach and determine who is responsible. It also will be a good idea to have law enforcement involved in this process. You obviously should not re-launch your online system until sufficient testing has been done to confirm that all vulnerabilities have been fully remediated. And before re-launching, your users should be validated (via email or otherwise) and instructed to change their account passwords before being able to log into your system anew. You also may want to undertake now to examine your system for obvious vulnerabilities, and to establish a data breach policy to follow in the event your system is compromised, so that you will have a prudent plan to follow should the need arise. You don't want to be in a situation where you need to haphazardly piece together such a plan in the wake of a data breach.

Another important item to consider is that your privacy policy can go a long way to mitigating the negative consequences of a data breach. If your privacy policy is drafted poorly, it can also be used against you in a potential lawsuit. We note that Sony's PlayStation Network privacy policy may have been updated subsequent to its recent data breach (the policy's "Last Revised" date states "April, 2011"). If this privacy policy was indeed revised after the data breach occurred, it is likely that whatever provisions Sony felt needed to be changed after the breach may very well be significant in determining what legal obligations Sony will have to its users.

Conclusion. A data breach can occur to systems employing even the most robust online security. The key for system operators is to respond to a data breach in a prompt and overall responsible manner. Be sure to know what all of your obligations are under the law and then comply with them fully and promptly. Finally, take protective steps now to protect yourself later, including a review of your data breach and privacy policies to ensure that these have been thoughtfully drafted and do not contain statements that may come back to haunt you.

For more information about responding to a data breach, and data security issues in general or any of the other items discussed in this Alert, please contact Baruch M. Bebchick at (646) 688-4375 or Email Us.

Strategic Ventures

Employment

Software

Marketing & Advertising

Entertainment

Trademark & Branding

Outsourcing

Biotech

Privacy

Business Formation & Reorganization

New Way to Avoid Class Action Suits

A recent Supreme Court decision, AT&T Mobility LLC v. Concepcion, No. 09-893 ("*AT&T v. Concepcion*") is being viewed by many legal experts as a game-changing ruling which will enable businesses to insulate themselves against customer class-wide arbitration actions and remedies. Many see this ruling as one of the most favorable pro-business decisions in quite some time.

In 2006, Vincent and Liza Concepcion sued AT&T for deceptive practices on behalf of a class of its consumers, because AT&T allegedly advertised discounted cell phones while charging sales tax on their full retail price. However, the agreements signed by customers with AT&T required that all claims be resolved through arbitration in an individual capacity, and expressly prohibited customers from seeking or participating in class-wide arbitration proceedings.

Both a California federal district court and subsequently the U.S. Ninth Circuit Court of Appeals held that the "no-class action" clause in the AT&T customer "arbitration-only" contract was contrary to California public policy and therefore unenforceable. This position by the Ninth Circuit conformed to the stance taken by courts in other jurisdictions over the past several years regarding "no-class action" provisions in contract arbitration clauses. Both the Second Circuit (which includes New York) and the Third Circuit (which includes New Jersey) have held in recent years that contract class action waivers were unenforceable in light of state law.

AT&T appealed the Ninth Circuit's decision, by arguing that that the Federal Arbitration Act trumps state contract law and permits a restriction on class action proceedings in arbitration. In *AT&T v. Concepcion*, the Supreme Court by a 5-4 vote, reversed the Ninth Circuit's ruling in finding that AT&T may indeed enforce contract provisions which prevent customers from banding together as a class in arbitration proceedings.

The *AT&T v. Concepcion* decision may have far-reaching implications in a wide range of business contexts. The decision presumably can be applied to a host of transactional relationships, whether internal to an organization (such as between a company and its shareholders or employees) or externally (such as between a company and its merchants or customers).

However, there is widespread speculation that Congress will intervene with legislation to trump *AT&T v. Concepcion* in order to reverse the decision's pro-businesses result. For example, the proposed Dodd-Frank Act calls for the Consumer Financial Protection Bureau to re-evaluate arbitration contract provisions which are deemed to be "anti-consumer".

How this all will play out is a matter of speculation about which various experts disagree, but what is clear is that *AT&T v.*

IP Management & Exploitation

Internet & e-Commerce

Media

Corporate & Commercial

Licensing

Strategic Ventures

Employment

Software

Marketing & Advertising

Entertainment

Concepcion has, at least for now, markedly changed the landscape of how businesses may insulate themselves from class-wide actions if they choose to limit disputes to resolution by arbitration.

Conclusion: In light of the Supreme Court's holding in *AT&T v. Concepcion*, you may want to consider revising the terms of various of your form agreements to require that all disputes be resolved through arbitration and to expressly prohibit the contracting parties from having any recourse to class action proceedings or remedies. You may now be able to ramp-up your level of protection in a way that would not have been likely to succeed prior to this recent Supreme Court ruling.

If you have any questions about finders or any of the items discussed in this Alert, please contact Baruch M. Bebchick at (646) 688-4375 or Email Us.

Trademark & Branding

Outsourcing

Biotech

Privacy

Bebchick Law offers a unique upside: the skill, quality and work ethic of a large New York firm with the personal attention and value of a small practice. By avoiding the overlapping and excessive overhead costs typical of many providers, we are able to deliver high quality legal services by experienced attorneys at well below the cost of other firms.

Our core practice involves corporate and intellectual property matters, with a focus on business formation & restructuring, IP management and exploitation, Internet & e-Commerce, media, licensing, employment, software, marketing & advertising, entertainment, branding, outsourcing, biotech and privacy. Bebchick Law regularly counsels clients about how to most effectively organize and reorganize, structure entrepreneurial ventures, and commercially protect and exploit their intellectual property and other assets.

We pride ourselves in bringing real value to our clients in an effective and efficient manner, by crafting practical solutions to legal and business problems and by providing sound advice on minimizing risk and avoiding pitfalls.

We invite you to learn more about us at Website.