2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

The Fallout of the Ashley Madison Attack

I. The Ashley Madison Debacle

Ashley Madison ("AM") was launched in 2001 and is a dating website marketed to people who are married or in committed relationships seeking to engage in adulterous behavior. The marketing campaign for AM included the tagline "Life is short. Have an affair". Due to the nature of the services offered, discretion and secrecy were (obviously) of significant importance to the company and the consumers it serviced. AM is owned by Avid Life Media, privately held Canadian corporation founded by CEO Noel Biderman.

On 7/20/15, hackers known as the Impact Team accessed and downloaded personal and financial info of more than $37M AM customers. The hackers threatened that if AM did not shut down, the hackers would release all the info in a "data dump". AM did not heed the warning, and on 8/18/15, a data dump of 9/7 gigabytes of highly sensitive info occurred. As a result, a list of the consumers that subscribed to the AM site was released. The list included many prominent individuals. In a message, the Impact Team allegedly stated "Too bad for ALM, you promised secrecy but didn't deliver."

The fallout of this data breach was widespread. It included alleged extortion attempts, suicides, and public humiliation. As a result, a number of class action lawsuits have been filed against the company including:

1. Canada: $578M Class Action in Canada (www.ashleymadisonclassaction.com); and,

2. U.S.: As of January 8, 2016, 36 lawsuits have been filed in the United States District Courts. Avid Life has filed a motion to consolidate.

The lawsuits allege, among other things, negligence, breach of contract and various privacy violations. Plaintiffs allege that AM failed to have adequate and reasonable measures in place to secure the data of users and failed to promptly notify users of the breach. There are also allegations that AM was aware of certain weaknesses in its computer systems. Additionally, in at least one lawsuit, it is alleged that AM made millions on $19 delete charges, and that at least some information remained on the site's databases.

AM is offering a $500,000 reward for information leading to the arrest and prosecution of the individual or group responsible for the breach.

According to media reports, American International Group, Inc. and Axis Capital Holdings LTD. provided at least some of the insurance available to AM. AIG allegedly provided directors & officers coverage while AXIS allegedly provided cyber insurance.

II. Cyber Liability

Cyber Crime

Cyber-crimes are criminal offenses committed via the internet that can occur both internally or externally to a computer network. Common examples of cyber-crimes are hacking, online scams, identity theft, email spam or phishing, and attacks on computer systems. Often, these data breaches can result in sensitive information such as consumer data and social security numbers being obtained. There are a variety of sources other than your typical hacker that can give rise to such data breaches such as disgruntled employees, negligent insiders, and cloud or third party compromises. As a result of the onslaught of data breaches, there is a need for cyberliability insurance policies to address the losses suffered.

Cyber Insurance

With the ever evolving sophistication and frequency of cyber-crime, cyberliability insurance policies are at the forefront to the breadth of risks and losses suffered by both the policyholder and third-parties. Cyber-crimes typically fall into either first-party or third-party losses. First-party policies respond to an insured for its own losses and can include commercial property policies, crime policies and fidelity bonds. Third-party insurance policies include commercial general liability policies (CGL), director and officer (D&O) policies, and errors and omissions (E&O) policies.

CGL policies traditionally provided coverage for wrongful acts arising from the performance of series as a technology professional or consultant. However, with the evolution of cyber based crimes, insurance policies have had to adapt to the gaps that exist in traditional coverage. Certain policies now cover a variety of expenses associated with data breaches such as: notification costs, credit monitoring, fines and penalties, costs to defend claims by state regulators, and loss resulting from identity theft. Additionally, third-party claims have now been implicating D&O and E&O policies. Specifically, shareholder lawsuits have been naming directors and officers in lawsuits for allegedly failing to ensure the appropriate procedures were implemented to prevent cyber-attacks. Additionally, E&O policies are implicated when claims assert that in the course of providing professional services, an organization’s negligence, mistake, omission, or error led to a data security breach. As cyber-crimes continue to change, cyberliability policies will have to respond with new forms and endorsements to address the continuous and new risks these crimes present.

III. Cybersecurity Information Sharing Act of 2015

As a result of cybersecurity threats, there was broad agreement that the nation's cyber defense posture could be greatly strengthened through more efficient and timely sharing of cyber threat information both between the government and the private sector and between private companies. The Cybersecurity Information Sharing Act (CSIA) of 2015 was recently passed by Congress and enacted into law right before Christmas. The bill requires the Director of National Intelligence and the Departments of Homeland Security, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities, nonfederal government agencies, state, tribal and local governments, the public, and entities under threats. CISA mitigates liability risks that may inhibit companies from sharing cybersecurity threat information. The goal is to promote voluntary information sharing.

IV. Examples/Cases

There have been a number of cases and incidents that resulted from various security breaches, including the AM hack. For example, in August 2015, a class action was filed in the U.S. District Court for the Central District of California styled *John Doe v. Avid Life Media (ALM), Avid Dating Life, Inc. dba Ashley Madison* (Case No.: 2:15-cv-060405-PSG-AJW). The case alleged that AM was negligent in properly securing personal information for users. AM offered its users a paid option wherein people who created a profile could have their account scrubbed from the website if they paid $19.00. However, not all information was scrubbed including GPS coordinates, city, state, DOB, weight, smoking/drinking preferences, gender, "what turns you on," and ethnicity.

Unfortunately there has been at least one suicide that occurred because of the AM hack. In Chicago, Donald Bradshaw took a fatal dose of prescription medication. His suicide note read that he was sorry for being unfaithful, that he knew he would be fired from his job, and that he would make it easy on his family by committing suicide.

In New Jersey, a fire was set by David Browne (a school district superintendent) to his home after he confessed to his wife and the school board that he had an AM account. He was charged with arson. Browne had been placed on administrative leave the same day of the fire in which he was injured.

The largest data breach at the time in 2007 involved TJ Maxx. In that breach over 45 million credit and debit card numbers were stolen over a period of more than 18 months. In addition, personal data provided in connection with returns of merchandise without receipts by about 450,000 people in 2003 was also stolen. As of March 2007, the company had spent over $5,000,000 in connection with the breach. Several lawsuits were filed against the company as a result of the breach.

A common email scam involves companies receiving emails from what they think are trusted clients. The email comes from the correct and known email address for the

client. The email requests two separate wire transfers and the wire instructions are contained on the proper form and are signed by the client. The wire transfers are executed. Ultimately, the signature is not the client's even though it looked like it. As of July 2015, similar scams had cost victims more than $1 billion in the previous 18 months.

In August 2014 JPMorgan Chase experienced a security breach where over 80 million customer accounts were stolen, which consisted of 76 million consumer accounts and 7 million small business accounts. The hacked data accounted for almost 65% of households in the US. After the hack was exposed JPMorgan Chase informed its customers that its breach was unlike other recent attacks on financial institutions, as there was no unusual fraud activity seen related to the incident.

Another famous security attack that occurred in the past year involved Sony Pictures Entertainment when Sony discovered internal documents, emails and movies had been leaked and that it no longer had control of its technology infrastructure. There are two theories about who attacked Sony, with North Korea and Russia at the forefront, in retaliation for the movie The Dictator. The Sony breach may have been one of the most scandalous attacks, but it was not as large scale as some of the other security breaches. Also, it was not the first time Sony was hacked as there were multiple data breaches which occurred in 2011 when Sony's PlayStation Network (amongst other products) were attacked. A settlement was achieved in this matter and Sony has agreed to pay its current and former employees as much as $4.5 million, with lawyers receiving $3.5 million, according to the settlement.

Wyndham Worldwide suffered three security breaches between 2008 and 2010 when hackers invaded the main network of one of Wyndham Worldwide's operating subsidiaries and stole information for over 619,000 Wyndham customers, mainly consisting of credit card information. After the breach Wyndham Worldwide was investigated by the Federal Trade Commission to determine whether Wyndham Worldwide engaged in deceptive or unfair acts or practices, including misrepresentations about security and unfair security practices that caused substantial injury to consumers. In addition to the FTC lawsuit, Wyndham Worldwide's shareholders demanded the board of directors bring a suit, but the board of directors declined. So instead, the shareholders brought a derivative suit against the board of directors. The Court followed the business judgment rule and dismissed the derivative suit, siding with the board of directors and indicating the board used its best and most reasonable judgment in meeting to discuss cyber security and proposed security enhancements on numerous occasions.

V. The Effects and Aftermath

JPMorgan Chase, Sony, Wyndham, and other companies hope to learn from the mistakes made in the prior security breaches and take proactive measures to stop an attack before it starts by eliminating information overload, reducing dwell time, and minimizing data loss exposure. It is prudent for security vendors, insurance carriers, practitioners, and technology officers to assess the risks involved and better develop products to combat these attacks.

These security breaches also serve to remind companies that when a data breach occurs, management needs to take a hands-on approach, be active in understanding potential cybersecurity issues, and participate in resolving problems after a breach. The Courts will generally show great deference to the boards in shareholder derivative actions when the directors and officers are actively involved in resolving the security issue. Directors and officers also need to review the company's insurance to assess cyber liability coverage and/or exposure. Directors and officers should also review the company's general liability and D&O insurance to determine whether cybersecurity breaches are covered, and if not, ensure that they have sufficient funding to respond to such a breach. Lastly, the board of directors should formulate an immediate response plan when there is a threat or potential breach of the system. The plan should include contacting both legal counsel and technical advisors and consultants who are well versed in the company's cybersecurity architecture and procedures to prepare to defend any potential lawsuits arising from the breach.