DannLaw urges victims of Marriott/Starwood date breach to preserve right to hold company accountable

Lodging company data breach exposes hundreds of millions to identity theft, consumer fraud

CLEVELAND, OHIO, UNITED STATES, December 3, 2018 /EINPresswire.com/ -- DannLaw, one of the nation's leading consumer protection law firms, is urging victims of the massive Starwood data breach to immediately take steps to both protect their personal information and preserve their right to seek financial compensation from the Marriott Corporation, Starwood's parent company.

Last week Marriott announced that sensitive information belonging to 500,000,000 million people who used the company's Starwood reservations system has been accessed by cybercriminals. According to the company the hackers copied names, addresses, dates of birth, passport numbers, email addresses, phone numbers, and encrypted credit card information from the Starwood reservation system. The company admits that the perpetrators may be able to overcome the encryption and use the credit card numbers.

"Starwood had a legal, ethical, and moral obligation to protect the information they obtained from consumers," Atty. Marc Dann said. "The company utterly failed to meet those obligations and now as many as 500 million people are at risk of having their identities stolen and their credit damaged or ruined by cyber criminals. They must be held accountable for their actions."

Atty. Dann noted that Marriott, like other companies that allowed customers' personal data to be compromised, waited months to reveal that the reservation system had been hacked. "Even worse, cybersecurity experts agree that the company missed multiple opportunities to detect and/or prevent the breach since it occurred in 2014," the former Ohio Attorney General said.

Those experts include Andrei Barysevich, a researcher with the security company Recorded Future Inc., who told the Wall Street Journal that a small breach the company suffered in 2015 should have set off alarms. "With all the resources they have, they should have been able to isolate hackers back in 2015," he said. Instead, hackers mined the company's reservation system for nearly four years.

"As a result, what could and should have been a minor problem has become one of the largest security failures in history," Atty. Dann said. "Whether willful or careless, it appears that Marriott

violated a number of consumer protection laws, and that means victims may be entitled to substantial compensation."

Anyone who used the Starwood system to reserve a room at one of the following properties in the past four years may be at risk:
- Sheraton Hotels & Resorts
- Four Points by Sheraton
- Westin Hotels & Resorts,
- W Hotels
- St. Regis, Element Hotels
- Aloft Hotels,
- The Luxury Collection,
- Tribute Portfolio,
- Le Méridien Hotels & Resorts, and
- Design Hotels.
- Starwood-branded timeshare properties

"Anyone who believes their personal or credit card information has been stolen should visit https://answers.kroll.com/, the website Marriott set up to deal with the problem and take advantage of the opportunity to enroll in WebWatcher for free," Atty. Dann said. "But please, do not agree to any waiver or release the company offers via email, regular mail, or via phone. The last thing a victim of the company's carelessness should do is surrender their right to hold Marriott accountable at a later date."

Atty. Dann also urged anyone whose data may have been compromised to arrange a free consultation with the firm's highly experienced legal team by calling 877-475-8100 or by completing the form that may be accessed at https://docs.google.com/.../1FAIpQLSfWi22blTFnoe5fLD.../viewform "We will be happy to walk people through the steps they need to take to preserve their rights under the law."

Finally, Atty. Dann suggested that potential victims take the following steps to protect themselves and their families:

Marriott is notifying impacted consumers by email. The email will come from starwoodhotels@email-marriott.com. When other companies provided notifications in this manner, cybercriminals sent fake emails asking individuals to provide information about themselves by providing links to fake websites or impersonating someone trusted. The email being sent by Starwood will not contain any attachments or request any information from consumers and links will only take recipients to the breach web site.

Check credit reports from Equifax, Experian, and TransUnion and look for any unauthorized entries or accounts.

Place a free credit freeze on your files. A credit freeze makes it harder for someone to open a new account in your name.

If you decide against a credit freeze, consider placing a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you;

Change your login information on your Starwood accounts. If you used that same username and password on other sites, change those as well;

Consider placing alerts on your financial accounts so your financial institution alerts you when money above a pre-designated amount is withdrawn;

Beware of potential phishing emails; don’t open email messages or attachments from unknown senders and do not click on any unknown links. Fraudsters will frequently send coercive and misleading emails threatening account suspension or worse if sensitive information is not provided;

Remember, businesses will never ask customers to verify account information via email or phone. If in doubt, contact the business in question directly for verification and to report phishing emails and phone calls; and

Be on the lookout for spoofed email address. Spoofed email addresses are those that make minor changes in the domain name, such as changing the letter O to the number zero, or lowercase letter I to the number one. Scrutinize all incoming email addresses to ensure that the sender is truly legitimate.

MARC DANN
The Dann Law Firm
+12164521028
email us here
