Brad D. Schimel
Wisconsin Attorney General

P.O. Box 7857
Madison, WI 53707-7857

NEWS FOR IMMEDIATE RELEASE

September 26, 2018

AG Schimel Reaches $148 Million Settlement with Uber over Data Breach; Settlements Funds to Establish Grant Program for Victims of Identity Theft

MADISON, Wis. – Attorney General Brad Schimel announced today that he, along with 49 other states and the District of Columbia, has reached an agreement with California-based ride-sharing company Uber Technologies, Inc. (Uber) to address the company's one-year delay in reporting a data breach to its affected drivers. Wisconsin will receive over $2.1 million. A portion of these funds will be used for a new grant program that will provide legal support to victims of identity theft and online fraud.

"Wisconsin entrepreneurs were made vulnerable by this data breach at Uber," said Attorney General Schimel. "While the company is taking direct action to ensure this never happens again, this new grant program will be there to provide legal support for Wisconsin victims of identity theft and data breaches in the future."

Uber learned in November 2016 that hackers had gained access to some personal information that Uber maintains about its drivers, including drivers' license information pertaining to approximately 600,000 drivers nationwide. Uber tracked down the hackers and obtained assurances that the hackers deleted the information. However, even though the breach of the drivers' license numbers for Uber drivers triggered Wisconsin law requiring them to notify affected Wisconsin residents, Uber failed to report the breach in a timely manner and waited until November 2017 to disclose it.

As part of the nationwide settlement, Uber has agreed to pay $148 million to the states. Wisconsin will receive $2,112,350.92. A portion of these funds will be used in a new grant program, administered by Wisconsin Department of Justice (DOJ) Office

DOJ Communications Office dojcommmunciations@doj.state.wi.us (608) 266-1221

of Crime Victim Services, to provide legal representation to victims of identity theft and online fraud.

In addition, Uber has agreed to strengthen its corporate governance and data security practices to help prevent a similar occurrence in the future.

The settlement between Wisconsin and Uber requires the company to:

- Comply with Wisconsin data breach and consumer protection law regarding protecting Wisconsin residents' personal information and notifying them in the event of a data breach concerning their personal information;
- Take precautions to protect any user data Uber stores on third-party platforms outside of Uber;
- Use strong password policies for its employees to gain access to the Uber network;
- Develop and implement a strong overall data security policy for all data that Uber collects about its users, including assessing potential risks to the security of the data and implementing any additional security measures beyond what Uber is doing to protect the data;
- Hire an outside qualified party to assess Uber's data security efforts on a regular basis and draft a report with any recommended security improvements. Uber will implement any such security improvement recommendations; and,
- Develop and implement a corporate integrity program to ensure that Uber employees can bring any ethics concerns they have about any other Uber employees to the company, and that it will be heard.

All 50 states and the District of Columbia are participating in this multistate agreement with Uber.

Attorney General Schimel offered the following tips Uber drivers or any consumers concerned about the security of their data can take after a data breach:

- Place a credit freeze on all of your credit reports. To place a fraud alert on your credit report, contact each of these three major credit reporting organizations.
    - Equifax https://www.alerts.equifax.com or call (800) 525-6285
    - Experian experian.com/fraud or call (888) 397-3742
    - TransUnion transunion.com or call (800) 680-7289
- Regularly request your free credit reports, inspect them closely, and promptly dispute any unauthorized accounts;
- Inspect all financial account statements closely and promptly dispute any unauthorized charges;

DOJ Communications Office dojcommmunciations@doj.state.wi.us (608) 266-1221

- 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 any 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. If in doubt, contact the business in question directly for verification and to report phishing emails; and,
- Be on the lookout for spoofed email addresses. Spoofed email addresses are those that make minor changes in the domain name, frequently changing the letter O to the number zero, or the lowercase letter l to the number one. Scrutinize all incoming email addresses to ensure that the sender is truly legitimate.

Wisconsin residents concerned about data breaches and what steps to take to further protect themselves, can find useful information at the Wisconsin Department of Trade and Consumer Protection's website.

DOJ Communications Office dojcommmunciations@doj.state.wi.us (608) 266-1221