IOWA DOT
SMARTER | SIMPLER | CUSTOMER DRIVEN
www.iowadot.gov

Motor Vehicle Division Informational Memo # 17-11

2017 Equifax Data Breach and Impact on Driver's Licenses and Identification Cards

DATE: October 2, 2017
FROM: Melissa Spiegel, Director, MVD
TO: All Driver and Identification Services (DIS) staff, Iowa County Treasurers and County Treasurers' staff that issue driver's licenses.

SUBJECT

This informational memo explains the announcement by the credit reporting company, Equifax Inc. and the Iowa Attorney General's office, that nearly 1.1 million Iowans may be affected by a recent data breach.

SUMMARY

That data involved in the breach includes social security numbers, birth dates, addresses and in some cases, driver's license numbers and credit card numbers. According to Equifax, the breach occurred mid-May through June of 2017, but that so far, the company has not found any evidence of unauthorized activity. The Iowa Attorney General's Office included a list of actions consumers can take to identify if their data has been compromised and also steps that consumers can take to guard against potential identity theft, all of which are included in the link to the press release below.

Customers are understandably alarmed by the recent news regarding the data breach, and since the information coming out, including from the Iowa Attorney General's Office indicates that driver's license numbers have potentially been exposed, customers have recently been contacting the DOT to inquire about how the breach impacts their driver's license (DL) or non-operator's identification (ID) number. Some customers have also inquired about the process for changing their DL or ID number.

Important Note: please be advised that at this time, the Iowa DOT has not been notified and has not received any indication that a breach of any DOT systems has occurred.

PRESS RELEASE

Please see attachment at the end of this memo.

CURRENT

We currently have the ability to change a customer's DL or ID number if the customer provides evidence that their DL or ID has been stolen. A police report is required to change the DL or ID number.

NEW

The current policy regarding changing a DL or ID number is geared towards situations where we know the customer's credential has been stolen and that can be proven by a police report. In the situation of a data

breach however, such as the Equifax data breach, we only know that a customer's personal information may have been exposed, but that is not the same thing as the data being compromised or knowing that your DL or ID number has been stolen. Changing DL or ID numbers can complicate our ability to effectively manage customers' identities. Therefore, if a customer is seeking to have their DL or ID number changed due to the Equifax data breach, or any other data breach, the customer will need to provide proof to us that their DL or ID number has been compromised and that it is causing them actual harm (not just potential harm in the future). Proof could include a police report or statement from another government entity or financial institution that identity theft activities have taken place involving the customer's DL or ID number.

BUSINESS IMPACT

This directive does not majorly change the way that DIS functions at this point in time, as we will continue to require customers who wish to change their DL or ID number to provide proof the credential has been compromised.

RESULT

It is important to be aware of the recent Equifax data breach and other data breaches where a customer's DL or ID number may be one of the items of personal information that has been potentially exposed, as customers will naturally come to us with questions about that type of data.

HELPFUL QUESTIONS AND ANSWERS

The following questions and answers provide additional information that will be helpful to you and to customers.

WHY CAN'T WE JUST CHANGE THE DL OR ID NUMBER IF THE CUSTOMER REQUESTS IT AS A PRECAUTIONARY MEASURE?

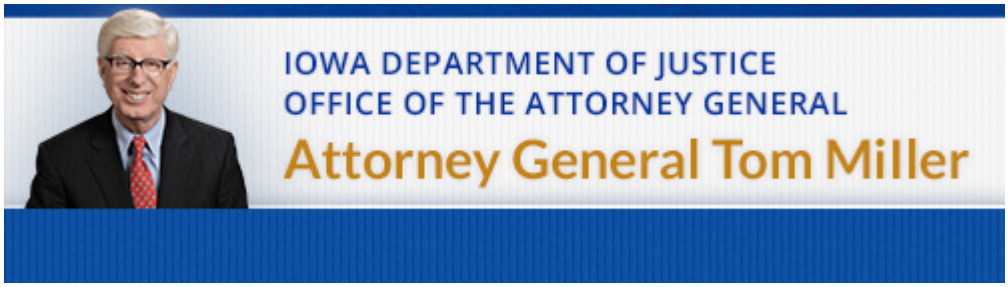
The customer's DL or ID number is used throughout multiple DOT systems, including the State Pointer Exchange Services (SPEXS) system and the Problem Driver Pointer System (PDPS) for out of state verifications, and therefore, changing a DL or ID number will cause records issues with these systems. That is why we should only be changing a customer's DL or ID number if there is evidence of some harm or they can prove it was stolen.

WHAT SHOULD WE TELL CUSTOMERS WHO CONTACT US WITH CONCERNS ABOUT THE DATA BREACH?

You may certainly let customers know that they have the ability to check with Equifax to determine if their data has been affected by the breach and that there are tips for them to monitor their accounts and receive free credit report monitoring. A good resource to provide to them would be the press release from the Iowa Attorney General's Office included at the end of this memo.

If the customer asks about having their DL or ID number changed, advise them that changing their assigned DL or ID number can complicate our ability to effectively manage their identity and that we will require proof that their identity has been compromised and that it includes their DL or ID number. Examples of proof can include a police report or statement from another government entity or financial institution that identity theft activities have taken place involving the customer's DL or ID number.

Skip to main content



Main Content

Latest Consumer Alert

September 12, 2017

Attorney General: Iowans Should Act Now Following Massive Equifax Security Breach

Miller opens investigation after credit reporting company discloses data breach affecting 1,099,125 Iowans

DES MOINES – Attorney General Tom Miller has opened an investigation into Equifax Inc. after the credit reporting company notified the Consumer Protection Division that nearly 1.1 million Iowans are affected by the massive data breach, which exposed personal information from approximately 143 million consumers nationwide.

The data involving 1,099,125 Iowans includes Social Security numbers, birth dates, addresses and, in some cases, driver's license numbers and credit card numbers.

The company disclosed that the breach occurred between mid-May through June, and that so far it has not found evidence of unauthorized activity.

"This data breach is astonishing, not only because of the number of consumers that it impacts, but also because of the key personal information that it exposed," Attorney General Tom Miller said. "Unfortunately, a criminal who gets a hold of this kind of personal information really hits the identity theft jackpot, and I'm concerned about the potential long-term impact this could have on countless consumers here in Iowa and across the country."

Miller urges all Iowans to check on whether the breach exposed their personal information. Equifax established a data breach website at www.equifaxsecurity2017.com. Consumers can run a simple check by entering in their last name and the last six digits of their Social Security number. The site will instantly display a message stating whether the breach exposed their

personal information.

Regardless of whether a consumer's information was exposed in the breach, Equifax is offering free credit report monitoring for one year. Consumers can enroll through November 21 for "TrustedID Premier" monitoring through the same site at www.equifaxsecurity2017.com.

Consumers with questions can also call an Equifax breach call center at 866-447-7559 from 6 a.m. to midnight, Central time.

"Our office is investigating the breach. We intend to hold Equifax accountable for what happened, and ensure that something of this magnitude never happens again," Miller said. "For now, though, our primary focus is helping and protecting Iowans affected by the breach."

Identity Theft Consumer Tips

- **Request and review your credit reports from all three credit reporting agencies (Equifax, Experian and TransUnion).** You can obtain each one for free once a year through a single website: www.annualcreditreport.com. You can choose to obtain all three at once, or you can stagger and rotate them throughout the year (one report from a different agency every four months).
- **Consider placing a security freeze on your credit report.** A security freeze locks out businesses from checking your credit report prior to opening a new account in your name. You can allow a credit check to proceed by providing a Personal Identification Number, and can stop the freeze at any time. You must contact all three credit reporting agencies separately for a credit freeze (one for each agency). The fee is $10 per agency for consumers who are not identity theft victims, which is a fee allowed by state law. Equifax announced it will waive security freeze fees for 30 days.
- **Consider an initial fraud alert.** If you suspect or confirm that someone stole your identity, an initial fraud alert can make it harder for an identity thief to open more accounts in your name. An initial fraud alert requires a business to verify your identity before issuing credit in your name. You only need to contact one credit reporting agency about an initial fraud alert, and that agency will notify the other two.
- **Monitor your accounts.** Review your statements and report any activity that is suspicious.
- **Be wary of breach-related scams.** Do not provide or "confirm" personal information to a caller who claims the call is related to the data breach, even if caller-ID information appears legitimate. Be wary of emails, which can be fake but look authentic, and be especially wary of clicking on links, opening attachments, or entering information on website addresses provided through emails or pop-up ads.

Consumers with questions or complaints can contact the Consumer Protection Division through our website at www.iowaattorneygeneral.gov, email us at consumer@iowa.gov, or call 515-281-5926 or toll-free at 888-777-4590 (outside the Des Moines metro area only).

For more information about identity theft, go to our website at www.iowaattorneygeneral.gov. To report and recover from identity theft, go to the Federal Trade Commission's site at www.identitytheft.gov.

###

For past consumer alerts, click here.
