**STATE OF NEVADA**

BRIAN SANDOVAL
*Governor*

DEPARTMENT OF BUSINESS AND INDUSTRY

C.J. MANTHE
*Director*

**FINANCIAL INSTITUTIONS DIVISION**

GEORGE E. BURNS
*Commissioner*

# Statement on Equifax Data Breach
September 12, 2017

Equifax, one of the three major consumer reporting agencies, recently announced a breach impacting an estimated 143 million U.S. consumers. The information accessed includes names, Social Security Numbers, birth dates, addresses and, in some cases drivers' license numbers. Credit card numbers for approximately 209,000 U.S. consumers were also accessed.

Fraudsters could use the stolen data for years to come to open fraudulent accounts and obtain loans. Financial institutions should alert staff to be cautious when opening accounts and processing loan applications.

The Nevada Financial Institutions Division believes that Nevada state-chartered financial institutions have maintained a strong information security posture, however, they need to be constantly vigilant. The Conference of State Banking Supervisors (CSBS) has been in touch with FS-ISAC (Financial Services-Information Sharing and Analysis Center) that is monitoring the situation for new information, including indicators of compromise and TTPs (Trust Transfer Process) that can possibly assist financial institutions to enhance their own defenses.

As a Nevada state-chartered financial institution, the data breach at Equifax affecting 143 million consumers was not your fault. The issue for our financial institutions is not what the hackers or Equifax did, or what they did not do, but rather what steps our financial institutions might not take into consideration in managing the consequences of the Equifax breach.

The 143 million consumers whose personal information was stolen are not Equifax's customers, they are the financial institution's customers. If Equifax is one of the financial institution's vendors, and in normal operations the financial institution provided Equifax with highly sensitive information that, if compromised, could cause significant harm to the very customers who trusted the financial institution with the personal identifying information (PII), part of the financial institution's responsibility was, and is, to perform rigorous due diligence and vendor management, to ensure that the PII is protected and now it is also the financial institution's responsibility to help its customers deal with this potentially damaging situation.

Financial institutions should be asking diligent questions regarding the Equifax data breach such as: What agreements does the financial institution have in place with credit bureaus and its customers regarding which party has liability in a breach of a credit reporting agency? What documentation in the vendor due diligence process did the financial institution depend on to evaluate and accept Equifax's security procedures? Was the financial institution's vendor due diligence systems assessment complete and

detailed or general and cursory? Will the financial institution continue sending PII to Equifax? What are the contractual implications?

Unfortunately, our Nevada financial institutions have had to deal with a number of data breaches over the years, both intrusions of their own systems and breaches of retailers that led to customers' credit or debit cards being compromised. Our Nevada financial institutions have developed pretty proven processes to identify impacted customers, monitor accounts and issue new cards as necessary. While customers find these breaches annoying and inconvenient, they generally trust their financial institution to do the right thing and protect them from fraudulent usage.

Nevada state-chartered financial institutions need to do whatever they can to provide assurances and confidence again with the Equifax breach.

Things financial institutions can do *(provided from regulatory and industry sources)*:

- **Patch Management** – Verify that all information technology and information security patches have been installed.

- **Confirm credit report information with your customers** – Before originating loans and before denying any loan, confirm credit report information with your customers.

- **Additional security measures –** If a customer informs you that they were one of the consumers whose information was stolen, you can code the customer account with a "red flag" to contact the customer at a pre-designated contact number or email prior to opening an account, applying for credit, or making any changes on existing accounts.

- Equifax reported a breach impacting roughly 143 million Americans. Unauthorized access occurred from mid-May through July 2017. The personal information accessed – names, Social Security Numbers, birth dates, addresses and, in some cases driver's license numbers – is everything fraudsters need to open fraudulent accounts. This could potentially result in fraudulent deposit losses from checks and ACH debits as well as ID theft- related loan fraud losses.

- Fraudsters could open fraudulent accounts in person at a branch; online account opening and online loan applications are particularly at risk since fraudsters prefer to avoid personal contact in branches.

- Use an identity verification/fraud service to verify the identity of individuals applying for new accounts or loans.

- Be alert for ID theft red flags on credit reports, including:

  - Notices of address discrepancy
  - Mismatched information (e.g., employment and birth dates) between applications and credit report
  - Fraud and Active Duty Alerts – the Fair and Accurate Credit Transactions (FACT) Act requires institutions to call the phone number listed in Fraud and Active Duty Alerts or take reasonable steps to verify the consumer's identity and confirm the application is not a result of ID theft
  - Be alert for a large number of recent credit inquiries

- Scrutinize individuals living outside of the financial institutions normal service area.

- Verify employment and don't rely on paystubs since they are easily manufactured. Instead, use a reliable phone number to verify employment.

- Perform a name and Social Security Number search to determine if accounts already exist on the system. Past ID theft related fraud schemes involved fraudsters who opened multiple accounts at a financial institution under the same name or Social Security Number.

- Use a robust identity verification solution for suspicious applications.

- Place extended holds on checks deposited to new accounts.

For online account opening financial institutions should consider these additional recommendations:

- Disable automatic approvals over weekends. These applications should require manual review.

- Require a manual review of applications for individuals who live outside of the financial institution's normal service area.

- Scrutinize IP addresses, including:

  - Geolocation tracking of IP addresses to ensure they are consistent with the individual's address
  - Be alert for multiple applications received from the same IP address
  - Block IP addresses if fraud is suspected. Note that fraudsters may quickly switch to different IP addresses after the block is in place

- Ensure the monetary limits are reasonable if customers can fund the account online (e.g., by ACH or payment card).

Equifax has established a dedicated website for consumers to determine if their personal information was impacted www.equifaxsecurity2017.com and to sign up for credit file monitoring and ID theft protection.

Consumers click the "Potential Impact" tab, enter last name and the last 6 digits of their Social Security Number. Consumers need to make sure they are on a secure computer and use an encrypted network connection. The website will let the consumer know if they have been affected by the breach.

Financial institutions could decide to notify customers of the Equifax breach and instruct them to visit the dedicated Equifax website to determine if their information was accessed. Inform impacted customers of their options for protecting themselves by placing a Fraud Alert on their credit file, placing a freeze on their credit reports, and monitoring their deposit and credit accounts for suspicious or fraudulent activity. In addition, remind customers of the importance of annually requesting and reviewing their credit report from the three major consumer reporting agencies.

The Federal Trade Commission has put out some steps to help protect consumers after a data breach:

- **Check your credit reports** from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don't recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do.

- **Consider placing a** credit freeze **on your files.** A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won't prevent a thief from making charges to your existing accounts.

- **Monitor your existing credit card and bank accounts closely** for charges you don't recognize.

- 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.

- **File your taxes early** — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Visit Identitytheft.gov/databreach to learn more about protecting yourself after a data breach.

If further information that will assist Nevada state-chartered financial institutions manage this Equifax data breach incident is forthcoming, it will be communicated.