STATE OF INDIANA **DEPARTMENT OF FINANCIAL INSTITUTIONS**

30 South Meridian Street, Suite 300
Indianapolis, Indiana 46204-2759
Telephone: (317) 232-3955
Facsimile: (317) 232-7655
Web Site: http://www.in.gov/dfi

GUIDANCE RELATED TO EQUIFAX DATA BREACH

TO: Indiana state-chartered financial institutions

FROM: Thomas C. Fite, Director
Chris Dietz, Deputy Director, Depository Division

DATE: September 22, 2017

Equifax, one of the major credit reporting agencies, recently announced a cybersecurity incident that is believed to have occurred between May through July 2017, potentially impacting an estimated 143 million U.S. consumers. According to its own investigation, Equifax reports that information accessed by criminals includes names, social security numbers, birth dates, addresses, and, in some cases, drivers' license numbers of consumers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

The Indiana Department of Financial Institutions ("the Department") is aware that many state-chartered financial institutions have a vendor relationship with Equifax, whereby the institution may both report and/or receive consumer credit information. Given the limited information at this stage that has been made available, as well as the highly sensitive nature of the personally identifiable information believed to have been compromised across a large number of consumers, and the high likelihood that information acquired would be abused and cause significant consumer harm, the Department is issuing the following guidance to Indiana state-chartered financial institutions to encourage pro-active steps for the benefit of the institution as well as Indiana consumers:

1. Ensure that all security updates and patches have been applied and are up to date on all core systems, web-servers, application firewalls, multi-function printers (which support a Web interface for configuration and management), and any other systems that store or transmit personally identifiable information;

2. Ensure that all policies and procedures concerning customer due diligence, ie, "Know your Customer", are being followed in a diligent manner by staff, whether for new or existing customers/members, for all account openings, credit cards, or loans issued;

3. As a result of the breach, many customers/members are likely to have credit freezes or fraud alerts placed on their credit reports - consider pro-active measures to train staff in how to utilize extra steps as necessary to verify an individual's identity and/or update the financial institutions' policies and procedures to include a consistent method on how to handle such circumstances;

4. If your institution is relying on information contained in Equifax credit reports as part of any consideration of extension of credit, consider taking extra steps to validate the information in the reports as well as an applicant's identity, as such information may have been compromised given this incident;

5. Heightened diligence should be exercised for new account openings or loan applications transacted exclusively through on-line methods;

6. Put a plan in place to determine how to immediately assist customers/members whose account at your institution has been compromised, including reissuance of debit and credit cards, and closing and re-opening accounts, as necessary;

7. Consider educating and encouraging your customers/members to take pro-active steps to protect their personal information.

Indiana's Security Breach Notification statute under Indiana Code Article 24-4.9 provides Indiana residents with a right to know when a security breach has resulted in the exposure of personal information, and we would anticipate that individuals will begin receiving such notifications within the coming weeks and will likely be contacting their financial institution for assistance. As a result, the Department strongly recommends that a financial institution take steps to ensure that staff is prepared to assist customers/members in the event that an individual's information is compromised.

The following are resources that may be of assistance to customers/members:

- FTC's IdentityTHeft.gov
- CFPB's Equifax data breach resource page, including "Top 10 ways to protect yourself in the wake of the Equifax data breach"
- Equifax's website