NEW YORK STATE
DEPARTMENT*of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Maria T. Vullo
Superintendent

September 18, 2017

To: To All Institutions Regulated by the Department of Financial Services

Guidance Relating to Equifax Data Breach

Equifax, one of the major credit reporting agencies, recently announced a cybersecurity attack impacting an estimated 143 million U.S. consumers. Although full information is not known, according to the reports of the incident, the information accessed by hackers includes names, social security numbers, birth dates, addresses, and, in some cases, drivers' license numbers of consumers. It has also been reported that credit card numbers of approximately 209,000 U.S. consumers have been accessed by hackers. The New York State Department of Financial Services (the "Department") is very concerned about this situation and will take all actions necessary and appropriate to protect New York's markets and consumers.

Unfortunately, the sensitive personal information apparently compromised by this attack is prone to significant abuse by criminals in opening accounts at financial institutions, or obtaining credit cards, loans, or other forms of financial services and products. This attack is particularly troubling as the number of affected consumers is incredibly high and the details have not been made known.

Given the seriousness of this breach and the potential harm to consumers and our financial institutions, and in light of the fact that a number of financial institutions have arrangements with Equifax under which financial institutions provide consumer and/or commercial related account and debt information to Equifax and also receive consumer and/or commercial related information services from Equifax, the Department is issuing this guidance to highlight the seriousness of this event and to ensure that this incident receives the highest level of attention and vigilance at your institution.

It appears that the hackers may have exploited a website application vulnerability to gain unauthorized access to very sensitive consumer and commercial data. However, the exact application vulnerability that was exploited is not known at this time. In the interim, the Department is issuing this guidance to urge New York State chartered and licensed financial institutions to consider the following:

1. Ensure that all information technology and information security patches have been installed;
2. Ensure that appropriate ID theft and fraud prevention programs are in place and followed for customer due diligence/Know Your Customer ("KYC") purposes and before an account is opened, or a credit card is issued, or any loan or other form of financing is approved, whether for new applicants or existing clients, and, if appropriate, consider using an identity verification/fraud service for identity verification;

3. Confirm the validity of information contained in Equifax credit reports (if you receive them) before relying on them for provision of products and services to new applicants, as well as existing clients, as they may have been compromised given the cyberattack;

4. If appropriate, consider a customer call center for customers to call in and inform your institution if their information has been hacked, in which case, consider coding the customer account with a "red flag" to contact the customer at a pre-designated contact number or e-mail address prior to opening an account, issuing a credit card, providing a loan or any other form of financing or other services and products, or making any changes to existing accounts; and

5. If your institution provides consumer or commercial related account and debt information to Equifax pursuant to any arrangement with Equifax, ensure that the terms of the arrangement receive a very high level of review and attention to determine any potential risk associated with the continued provision of data in light of this cyberattack, taking into consideration the Department's cybersecurity regulation (23 NYCRR Part 500) with respect to third party service providers.

This incident once again highlights the fact that financial institutions can no longer just rely on personally identifiable information ("PII") as a means of verifying a person's identity as, unfortunately, we are confronted with an environment where PII is being bought and sold as a result of events such as this incident, which increasingly necessitates consideration of Multi-Factor Authentication and Risk-Based Authentication techniques, as encouraged under the Department's cybersecurity regulation.

Sincerely,

Maria T. Vullo
Superintendent