Equifax Data Breach: A Bank's Role

Written by Lauren C. Capitini
Boardman & Clark
09.20.17

As all banks are now aware, Equifax, one of the three major credit bureaus, was hacked between mid-May and July 29, 2017. The incident potentially impacts the personal information of 143 million U.S. consumers (roughly half the U.S. population). Specifically, names, social security numbers, birthdates, addresses, and in some instances, drivers' license numbers and credit card numbers, were compromised. Though the breach originated at Equifax, Wisconsin banks will inevitably be impacted due to a vulnerable customer population. So, what is a bank required to do when its customers have been impacted by an indirect data breach?

First and foremost, banks are not legally required to notify customers of a third party (non-service provider) data breach. That said, any proactive steps a bank can take to notify customers of their rights and responsibilities could mitigate risk for both the customer and the bank. For example, a bank should encourage customers to monitor their accounts, review their account statements, and report any unauthorized activity to the bank as soon as possible, but certainly within timeframes established by federal law to limit customer liability (e.g. for unauthorized ATM or debit card activity, 60 days from receipt of the periodic statement on which the alleged error is reflected). Additionally, banks could benefit from providing information related to the breach itself, including how customers can request a credit freeze or fraud alert be placed on their credit report. *

Second, to the extent a bank has developed a process to respond to a third-party data breach, the bank should follow those procedures, as appropriate. This may include, for example, monitoring customer accounts for unusual activity and issuing new debit and/or credit cards, as appropriate. As it relates to the issuance of new debit or credit cards, Bankers' associations have requested Equifax notify all affected card issuers if their customers were among the 209,000 individuals whose credit or debit card information was exposed. In addition, we understand that VISA and Master Card have reached out to financial institutions related to the breach; to the extent you have not been contacted by Equifax or your card provider, we suggest proactively reaching out to them directly to ascertain whether or not the Bank will be notified if its customers are affected.

Additionally, if a customer reports fraud or unauthorized activity on an account, a bank must comply with federal regulations, as delineated in Regulation E (for debit card, ATM card, and other electronic fund transfers) and Regulation Z (for credit cards and other types of open-end credit). For example, if a customer discovers unauthorized ATM or debit card activity, Regulation E requires it be reported to the bank within 60 days of receipt of a periodic statement on which the alleged error is reflected. A bank must then investigate and determine whether an error occurred within 10 business days. That 10 business days can be extended to 45 or 90 days in certain circumstances. A bank must notify customers and correct errors within certain timeframes, as well.

Finally, a bank should heed any fraud alerts on an applicant's credit report by taking steps to reasonably verify the identity of such applicant before extending new credit (other than pursuant to an existing open-end account), issuing an additional card on an existing credit card account, or increasing a credit limit on an existing account. Banks should comply with these Fair Credit Reporting Act responsibilities as well as any applicable policies and procedures. Importantly, because the Equifax breach potentially compromised a broad range of customer identifying information, a bank should reconsider whether the data it currently uses to "form a reasonable belief" that the bank knows the customer's identity is sufficient or if alternative data points should be used. For example, if a bank typically uses a social security number or address to verify a customer's identity in the wake of a fraud alert, this may be insufficient given that this type of information was compromised in the breach. The bank could, instead, verify an

email address and location where the account was opened, for example. A bank may also consider updating applicable policies and procedures accordingly. In addition, banks should stand ready to answer questions from customers regarding the lifting of a credit freeze.

As we know, Equifax was not the first and it will not be the last data breach to impact your customers. It is prudent that banks take these steps, as appropriate, to protect themselves and their customers.