LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Assessing Loan Applications With Fraud Alerts After Equifax

By **Jonathan Joshua** (September 28, 2017, 10:44 AM EDT)



Jonathan Joshua

In early September, Equifax announced that it had been the victim of hackers who had accessed the personal information of up to 143 million consumers.[1] In the wake of this data breach, the Consumer Financial Protection Bureau[2] and many experts are advising consumers to place fraud alerts or credit freezes on their accounts.[3] As a result, consumer lenders can reasonably expect to see a significant increase in the number of loan applications in which an applicant's credit report contains a fraud alert or where the credit report is unavailable as the result of a consumer's security freeze. It is important to understand the laws that apply when evaluating such loan applications.

Fraud Alerts

In 2003, the Fair and Accurate Credit Transactions Act (FACTA)[4] was enacted to "expand access to credit and other financial services for all Americans, enhance the accuracy of consumers' financial information, and help fight identity theft."[5] In relevant part, FACTA amended the Fair Credit Reporting Act to add a new section allowing consumers to place on their credit report two types of fraud alerts, an "initial alert" and "extended alerts."[6]

Initial Alerts: Initial Alerts can be requested by a consumer (or an individual acting on behalf of a consumer) "who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft ..." Upon receipt of an initial fraud alert, a credit reporting agency must include the initial fraud alert in the consumer's credit file and notify the other credit reporting agencies of the fraud alert. The credit reporting agency must also provide to the consumer a free copy of the consumer's credit report.

Extended Alerts: Upon submission of an identity theft report (which includes a law enforcement report or an affidavit of fraud that is made under the penalty of perjury) to a credit reporting agency, the credit reporting agency must maintain an extended fraud alert on the consumer's file for seven years following such request. The credit reporting agency must also exclude that consumer from lists intended for pre-screened offers of credit and must notify the other credit reporting agencies of the extended fraud alert.

"Clearing" Fraud Alerts

Potential creditors who receive a fraud alert from a credit reporting agency in connection with a consumer's application for credit should seek to "clear" the fraud alert as required by law.

- **Initial Alerts:** A user of a credit report which contains an initial fraud alert may not establish any new credit plan or extension of credit (other than an open-end plan of credit), or issue an additional card on an existing credit account, or grant any increase in credit limit on an existing credit account, "unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request." Furthermore, if the initial fraud alert "has specified a telephone number to be used for identity verification purposes," then the creditor must "contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the

application for a new credit plan is not the result of identity theft."

- **Extended Alerts:** A user of a credit report which contains an extended fraud alert may not establish a new credit plan or extension of credit, other than under an open-end credit plan, in, or issue an additional card on an existing credit account, or any increase in credit limit on an existing credit account requested by a consumer, "unless the user contacts the consumer in person or using the telephone specified by the consumer in the fraud alert for identity verification purposes to confirm that the application for a new credit plan or increase in credit limit, or request for an additional card is not the result of identity theft.

The primary difference between resolving an initial fraud alert and an extended fraud alert is that an initial fraud alert may be cleared if the prospective creditor either contacts the consumer at the specified telephone number (if any) or if the creditor takes reasonable steps to verify that the application is not the result of identity theft. In contrast, to clear an extended fraud alert, the prospective creditor must either contact the consumer "in person" or using the specified telephone number (if any).[7]

The precise nature of the "in-person" requirement for clearing an extended fraud alert is undefined and may be problematic under various circumstances, such as in connection with an indirect auto finance transaction or a point-of-sale financing transaction.

Credit Freezes

Credit freezes are mandated by the laws of 47 states (and offered voluntarily by the credit reporting agencies in the other states).[8] Broadly speaking, credit freezes prohibit the credit reporting agencies from providing a copy of a consumer's credit report to any third party after the consumer follows the applicable procedures to institute a credit freeze. Creditors who receive applications from consumers but are unable to obtain a credit report due to a credit freeze should contact the consumer directly and request that the credit freeze be lifted with respect to the consumer's application for credit. The consumer must then work with the credit reporting agencies to lift the freeze, after which the creditor may re-request the credit report.

Evaluating Applications for Credit in the Presence of a Fraud Alert or Credit Freeze

Creditors should use the various methods discussed above to confirm the legitimacy of an application for credit. Significantly, the existence of a fraud alert or credit freeze does not extend the potential creditor's 30-day time limit to notify the applicant of the creditor's decision on the application.[9] On the other hand, a potential creditor who rejects an application out-of-hand solely because the applicant has a fraud alert on his or her credit report should consider its potential exposure to liability under the Equal Credit Opportunity Act's prohibition against discrimination against a consumer who has exercised any right available under the Consumer Credit Protection Act (15 USC 1601 et. seq.). See, 15 U.S. Code § 1691(a)(3).

Finally, note that following these procedures does not excuse a financial institution from maintaining a strong identity theft prevention program to detect, prevent and mitigate the effects of identity theft, as required by FACTA and the implementing "Red Flags" regulations.[10] The lack of a fraud alert or credit freeze is likely not dispositive as to the legitimacy of an application for credit.

Jonathan Joshua is a consumer financial services attorney in New York. He advises clients about the laws and regulations of consumer lending and privacy, with an emphasis on student loans, auto loans and personal loans.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[2] See, https://www.consumerfinance.gov/about-us/blog/top-10-ways-protect-yourself-wake-equifax-data-breach/

[3] See, e.g., https://www.consumerreports.org/credit/how-to-freeze-your-credit-while-applying-for-loan/ and https://www.usatoday.com/story/money/2017/09/11/how-defend-yourseafter-equifax-data-breach-credit-report-freeze-strong-defense-against-identity-thef/654065001/

[4] Public Law 108–159, Dec. 4, 2003.

[5] See, White House Fact Sheet, Dec. 4, 2003, at https://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031204-3.html

[6] 15 USC 1681c-1

[7] Note that the use of autodialing equipment to initiate telephone calls to consumer's cellular telephones without the prior express consent of the called party may pose risks under the Telephone Consumer Protection Act, 47 U.S.C § 227. While the FCC exempted autodialed calls to cellular telephones which are "intended to prevent fraudulent transactions or identity theft," the applicability of such exemption to clearing fraud alerts is unknown. See, Paragraph 129, FCC Omnibus Declaratory Ruling and Order, DA/FCC: FCC-15-72, June 18, 2015.

[8] See, e.g., https://www.consumerfinance.gov/ask-cfpb/what-does-it-mean-to-put-a-security-freeze-on-my-credit-report-en-1341/

[9] 12 CFR §1002.9.

[10] 16 CFR Part 681.

All Content © 2003-2023, Portfolio Media, Inc.