OCCC
TEXAS OFFICE OF CONSUMER CREDIT COMMISSIONER

Advisory Bulletin to All Licensees & Registrants: Information Security After the Equifax Data Breach

The recent Equifax data breach affected 143 million Americans, including nearly 12 million Texans. Hackers accessed names, birth dates, addresses, Social Security numbers, driver's license numbers, and credit card numbers.

This bulletin summarizes three significant requirements for OCCC licensees and registrants after the Equifax data breach:

- Fraud alert restrictions under the FCRA
- Identity theft prevention programs under the FTC Red Flags Rule
- Information security programs under the FTC Safeguards Rule

This bulletin also has links to resources that can help creditors prevent identity theft and protect consumers' information.

This bulletin is just a summary. Licensees and registrants are responsible for ensuring that they comply with all applicable laws, not just the laws listed in this bulletin.

1. FCRA fraud alert restrictions

Under the Fair Credit Reporting Act (FCRA) and state law, consumers have the right to place a fraud alert or security freeze on a credit report:

- A fraud alert requires creditors using the credit report to verify the consumer's identity before opening a new credit account. FCRA, 15 USC 1681c-1.
- A security freeze prohibits a credit bureau from releasing a credit report without the consumer's authorization. Tex. Bus. & Comm. Code 20.01(8), 20.034.

A fraud alert restricts a creditor from creating a new account in the consumer's name. If a consumer has a fraud alert on a credit report, a creditor using the report may not establish a new credit account or extension of credit, unless the creditor has reasonable policies and procedures to determine the identity of the person requesting the new account or extension. FCRA, 15 USC 1681c-1(h)(1)(B)(i).

After the Equifax data breach, many consumers are placing fraud alerts, security freezes, or both on their credit reports. The OCCC encourages creditors to work with consumers. Creditors may need to take additional steps to verify the consumer's identity (e.g., calling the consumer), and may need to allow the consumer to temporarily lift a security freeze.

2. FTC Red Flags Rule

The Federal Trade Commission's Red Flags Rule, 16 CFR pt. 681, requires creditors and financial institutions to develop and follow an identity theft prevention program.

The program must include policies and procedures to:

- identify red flags for covered accounts,
- detect red flags,
- respond to red flags to prevent and mitigate identity theft, and
- ensure that the program is updated periodically to reflect changes in risks.
  FTC Red Flags Rule, 16 CFR 681.1(d)(2).

A red flag is a pattern, practice, or activity that indicates the possible existence of identity theft. Examples vary based on the type of business, but the FTC has identified five general categories of red flags:

- alerts from credit bureaus (e.g., fraud alert, notice of security freeze),
- suspicious documents (e.g., identification looks altered or forged, information differs from what a person is saying),
- personal identifying information (e.g., inconsistencies in information, same information used by a known fraudulent account, same address used by multiple applicants, inability to answer challenge questions beyond what is typically in a credit report),
- account activity (e.g., requesting new accounts shortly after an address change, account used outside of established patterns, inactive account is used again),
- notice from other sources (e.g., statements that account was opened or used fraudulently from consumer, identity theft victim, law enforcement, or someone else).

Identity verification and authentication methods can help creditors detect red flags and prevent identity theft:

- For online transactions, the methods could include calling the consumer with a designated phone number before approving or denying loans, or the use of two-factor authentication to log in to an account page.
- For in-person transactions, the methods could include training employees on how to check government-issued identification such as a driver's license.
- Creditors should consider procedures for both new accounts (when a consumer is applying for the first time) and existing accounts (when a consumer is making changes to an account or applying for another extension of credit). After the data breach, identity thieves may attempt to use stolen information to obtain advances on existing accounts.
- Creditors should ensure that their software includes any security-related updates.
- When creditors detect red flags, they should be prepared to respond appropriately. This could include contacting the consumer, changing an account password (or other method of accessing an account), closing an account, and notifying law enforcement.

A creditor should tailor its identity theft prevention program to its particular business model. The creditor should document the program in writing and train employees on it. The creditor should also update its program periodically to ensure that it stays up-to-date with any changing business practices and new methods of identity theft.

Additional information on developing an identity theft program is available at:

- FTC—Appendix A to the Red Flags Rule
- FTC—Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

3. FTC Safeguards Rule

The FTC Safeguards Rule, 16 CFR pt. 314, requires financial institutions to develop, implement, and maintain an information security program, to ensure security and confidentiality of consumer information.

As part of the information security program, the financial institution must:

- designate an employee to coordinate the program,
- identify risks in all areas of operations,
- design and implement information safeguards and regularly test them,
- oversee service providers to ensure they have appropriate safeguards, and
- evaluate and adjust the program based on testing and monitoring.
  FTC Safeguards Rule, 16 CFR 314.4.

As with the identity theft prevention program, the information security program should be tailored to an institution's particular business model. The institution should document the program in writing and train employees on it. The institution should update the program periodically to ensure that it stays up-to-date with any changing methods of storing consumer information.

Additional guidance on developing an information security plan is available on the FTC page: Financial Institutions and Customer Information: Complying with the Safeguards Rule.

4. Additional information about the Equifax data breach and other data breaches

- Texas Attorney General—Equifax Data Breach Affects Nearly 12 Million Texans
- FTC—The Equifax Data Breach: What to Do
- FTC—Data Breach Response: A Guide for Business
- FTC—IdentityTheft.gov: When Information Is Lost or Exposed
- CFPB—Identity Theft Protection Following the Equifax Data Breach