

The FACT Act: Gains for Consumers, Potential Liability for Businesses

by Dr. Linda Eagle

Identity theft has been on the rise in recent years. It is virtually an undetectable crime, whereby a thief steals the identity of an unsuspecting victim by obtaining vital personal information such as their name, address and most critically, their social security number. Then cloaked in this false identity, the thief proceeds to obtain credit, loans, false bank accounts and rack up debt in the victim's name. Like the proverbial thief in the night, he disappears, leaving the consumer with a mess to clean up, and the affected businesses scrambling to minimize financial damages and liabilities.

The federal government has responded to this increase in illegal activity by writing the *Fair and Accurate Credit Transaction Act of 2003* (FACTA), an amendment to the *Fair Credit Reporting Act* (FCRA). FACTA, also known as the *FACT Act*, calls for credit reporting and receiving agents to impose stricter guidelines on information accuracy and privacy, limits information sharing, and provides more rights for consumers. Since 2003, updates to the Act have been made in order to combat the rise of this dangerous crime.

The FACT Act establishes:

- Fraud alerts
- Truncation of account numbers
- Procedures to identify risks
- Truncation of social security numbers
- Identity theft rights
- Free credit reports
- Credit score disclosures
- Opt out rights
- Sharing of credit reports
- Disposal of consumer report information
- Negative information disclosures
- Risk based pricing notices
- Increased accuracy of credit records
- Consumer complaint procedures
- Improved reinvestigation
- Reconciliation procedures
- Dispute procedures
- Medical information protection

The Benefits to Consumers

Credit bureaus, a group of agencies that gather and distribute consumer credit data including personal and debt repayment information, traditionally charge a fee for a personal credit report ordered by the consumer. Due to the rise in identify theft, the government has now made it possible for consumers to monitor what is being reported about them, free of charge. For a nominal fee, consumers may also request their credit score, including an explanation of how the score was calculated.

If a consumer does become the victim of identity theft, FACTA provides additional privileges. The Act allows victims to require that credit bureaus attach a “fraud alert” to their credit profiles. Military personnel may place a specific alert to their profiles, indicating to any potential creditor that the individual is an active duty serviceperson, and therefore may not be the actual applicant of any new loan, credit card or account.

FACTA also makes provisions for credit reporting agencies to conceal the identity of a medical provider that is reporting past due bill repayment, so that a potential creditor or employer will not inadvertently discover the medical condition of the borrower/applicant.

The Responsibility of Businesses

On October 1, 2008, FACTA made it mandatory for businesses such as merchants or bank ATMs that issue credit or debit card receipts, to print only the last five digits of the card number or expiration date. This requirement will help provide better protection against identity theft for consumers.

Financial institutions are subject to more procedural requirements thanks to FACTA. The burden is on the furnishers of data to credit reporting agencies to ensure that the data they are providing is accurate. As of January 1, 2008, financial institutions are required to adopt procedures that will detect fraud and identity theft before it occurs, or recognize “red flags.” These red flags may be a suspicious change of address request, a request for a duplicate debit or credit card, or the reactivation of a dormant card. Financial institutions and creditors must comply by November 1, 2008.

Businesses that offer credit must also provide victims of identity theft with copies of false applications and other documentation upon the victim’s request. However, there are some exceptions to this requirement in place to protect the credit-offering company from a false theft claim. Additionally, banks and other credit-offering businesses are required to notify applicants of less desirable pricing when the consumer has been solicited for a loan at one price, but after a credit investigation reveals a low credit score, are then offered a higher price or interest rate for the loan. Such notification enables the consumer the opportunity to question a false low credit score — a possible result of credit fraud or identity theft.

Notably, FACTA requires businesses to destroy all personal information on consumers, clients, and employees before discarding it. Businesses must protect against unauthorized access to or use of the information in connection with its disposal. The law allows for civil liability, and courts are authorized to award punitive damages and attorney’s fees through an individual or class action suit. State and federal fines can be excessive for any breach.

Finally, FACTA expands the “opt out” provisions outlined in FCRA for information sharing for marketing purposes among business affiliates. Since direct marketing-related list sharing multiplies the number of places a consumer’s data appears, it thereby increases the risk of unauthorized access, leading to potential identity theft.

At this point, the judiciary has generally rejected victims' tort claims against businesses accused of enabling identity thieves. However, given the increased occurrence of identity theft-related crime, the tide could change. The claim of "negligent enablement of an imposter" has already been recognized by the Alabama courts. In *Patrick v. Union State Bank*, the Alabama Supreme Court held that when a bank opens an account in a person's name using his identification, the bank owes a duty of reasonable care to that person to ensure that the individual opening the account and presenting the credentials is not an imposter.

The Final Word

The struggle of maintaining a fair balance between consumer protection, and the sales and marketing efforts of financial organizations is an age-old problem. The federal government's response to this rise in unconventional crime by instituting a more controlled method of handling consumer information is one way of protecting both sides. However, in a world of clever and innovative thieves, financial institutions need to stay one step ahead to ward off potentially damaging liability suits. Therefore, it's to the best interest of financial institutions to stay abreast of the continuous progress and application of this law.

Good Practice Guidelines:

- 1) Ensure that your business practices adhere to the Act's requirements applying to consumer reporting agencies, companies that furnish data to those agencies, and those who use information provided by those agencies.
- 2) Adopt reasonable business standards for the secure disposal of sensitive consumer data.
- 3) Store all business records containing sensitive information in a secure location to prevent unauthorized access.
- 4) Shred, pulp or burn all documents that contain identity information that the business is not required by law or policy to retain.
- 5) Create and maintain reasonable operating procedures to ensure that information about individuals is reported with maximum accuracy.
- 6) Watch for trends in federal and state court rulings holding businesses liable in facilitating an identity thief's commission of a crime.
- 7) Monitor legislative developments regarding identity theft since consumers are quick to pressure their legislators for protections as cases arise.

Dr. Linda Eagle is Founder & President of The Edcomm Group Banker's Academy—a 21-year-old education and consulting firm dedicated to serving Banks, Credit Unions, Money Services Businesses and all areas of the Global Financial Community with thousands of generic and customized training programs in areas such as BSA/AML, Regulatory Compliance, Teller Training, Systems Training, Sales and Service Training, and many more.

[Edcomm Banker's Academy](http://www.edcomm.com) is headquartered in New York, NY. For more information, email linda.eagle@edcomm.com or call 888.433.2666/+1.212.631.9400.