Inquesta Corporation

Email: admin@inquesta.com

Website: www.inquesta.com

Identity Theft Prevention

Jacques R. Island

Email jisla@inquesta.com

The scourge of identity theft didn't just start in 2003 when the Fair and Accurate Credit Transactions (FACT) Act (FACTA) was finally passed to address a problem that had been in the making at least since 1982[1] (when the author testified as a federal agent before the U.S. Senate about federal identification fraud). It has been a problem as long as drug trafficking, modern-day terrorism, Medicare and bank cards have been around. But the growing menace was still a submerged iceberg then.

Frauds using stolen identities once took practiced criminals. Since the Internet, computers, sharp color copiers, swipe cards, and ATMs, to name just a few of the facilitators, the floodgates to fraud have been opened to just about anyone inclined to crime.

Worse, the Internet has torn down physical and international boundaries such that the worst of the identity thieves stealing U.S. consumers' lives don't operate from the U.S. at all; they operate from third world havens…out of reach to U.S. law enforcement and perpetrating their harm from a safe distance. The long-running "Nigerian scams" are among the best known examples of this.

According to U.S. Government statistics, there were **10.8 million identity theft victims in 2003**, making this the fastest-growing white-collar crime in the U.S. in 2003.

FACTA—in combination with improving technology, better consumer education and the individual efforts of a growing number of creditors—has driven the numbers of identity theft victims down to **8.1 million victims per year by 2007**. This is still a tremendously large fraction of the population even if the numbers have been in a slow decline since 2003.

On the financial side, consider that identity theft costs U.S. consumers and creditors more than **$50 billion in losses per year**.

The decline is welcome but there's so much left to do…and FACTA is the trigger that has galvanized the financial sector into concerted action. Still, we cannot let up our guard as the identity criminals are forever looking for newer angles and finding holes in the technology.

What the FACT Act is

After decades of hearings and inaction, Congress finally passed the FACT Act in 2003 specifically to battle identity theft and to ease the burden of victimized consumers needing to correct their credit histories. Generally, the intent of the Act is threefold, to:

- require *consumer reporting agencies* (CRAs) to stop attributing to the credit history of a consumer complainant information that the consumer demonstrates to be erroneous or fraudulent;
- require creditors or businesses to provide copies of documents that pertain to a complainant of identity theft so they may challenge the transaction and cause it to be removed;
- allow consumers to report directly to creditors as well as the CRAs those accounts affected by identity theft, to prevent the spread of erroneous credit information.

To accomplish these goals, the Act mandates the following general provisions:

---

[1] U.S. Senate, Hearings before the Subcommittee on Investigations of the Committee on Governmental Affairs. *Federal Identification Fraud.* 97th Congress, 2nd session, June 15 and 16 and September 28, 1982.

- The big three credit bureaus (Expirion, Equifax and Trans Union) now must provide each requesting consumer a free copy of the consumer's credit report at least once per year so that consumers can analyze the report for inaccuracies or falsehoods to challenge and have removed from the record.
- It established a National Fraud Alert System (database) into which consumers can place alerts that they have been victimized or think they may be victimized. This system's purpose is to alert creditors to proceed with caution in granting credit in the presence of an alert.
- Creditors and businesses are required to truncate account numbers that can be used for fraud.
- Creditors and businesses holding consumer information must use reasonable document disposal practices.
- CRAs (including resellers) must notify consumers of their rights under the FCRA.

In October 2007, the Federal Trade Commission (FTC) and Federal Reserve Board expanded on the law and issued a new, mandated requirement to the FACT Act—the Red Flags Rule—to be implemented by each financial institution or creditor by no later than November 1, 2008.

Red Flags Rule: The Immediate Compliance Issue

Many financial institutions have already implemented those portions of the initial FACTA regulations that address identity theft and may already have a semblance of an Identity Theft Prevention (ITP) program or a Customer Identification Program (CIP). But adding the Red Flags Rule guidelines produces a more secure system; one that scrutinizes, at a minimum:

- which of the institution's accounts are subject to identity theft;
- how the accounts at risk are opened;
- how the accounts at risk are accessed;
- the size, location and customer base of the institution; and,
- the institution's previous experiences with identity theft;

with each of these serving as an element in the conduct of a **risk assessment**.

The risk assessment, in turn, serves as the basis for building the company's ITP program to the standards of the Red Flags Rule.

Flexibility in Establishing a Red Flags Rule Program

The FTC recognizes that many institutions have been diligent in establishing effective programs that address their own needs. Thus, the new mandate provides for flexibility in implementing a *risk-based* program that suits each institution's (1) unique needs and (2) best practices to control "reasonably foreseeable" identity theft risks.

Other Related Laws and Programs to Blend With

Congress has been incremental in passing laws to protect private information; thus, there are overlapping requirements in existing laws, but FACTA sets new standards for consumer information protection. Each of the laws should be kept in mind during a FACTA risk assessment to assure that the business produces a cohesive program to protect private information from theft. The other laws are:

- The Identity Theft and Assumption Deterrence Act of 1998 that made the FTC the central repository for identity theft complaints and assistance of victims.
- The Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act (GLBA), which requires that banks protect private information from foreseeable threats and criminalizes pretext calls, now commonly known as "*social engineering*".
- The Bank Secrecy (BSA) and The Patriot Acts, both of which require a customer identification program (CIP), often referred to as "Know Your Customer" or KYC requirement. They are substantially different from the intent of the FACT Act. Nonetheless, they have similar implications for storing and protecting private data.

These different yet related laws should be considered holistically within the business so that they are dovetailed within its written procedures. The Red Flags Rule assessment and procedures should not be developed and implemented in isolation of the others.

FTC Requirements as Our General Objectives

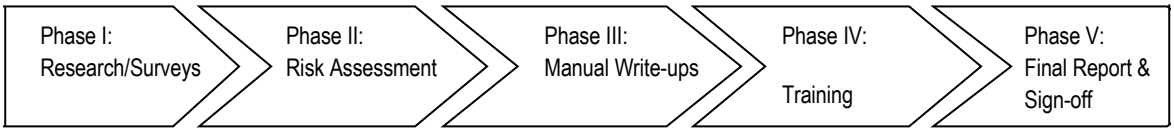
In addition to what consumers can do for themselves, consumers' best protection against identity theft is with the repositories of their personal data: the banks, retail companies, universities, utility companies, and myriad similar institutions that have a legitimate need to collect and hold consumer information. These entities must now take stringent measures to protect consumer information from unauthorized persons or impermissible uses. Generally, the FTC's Red Flag Rule mandate is to:

- Heighten awareness and implement a **written identity theft prevention program** that
  - detects, prevents and mitigates ID theft, and
  - suits the institution's size, complexity and nature of its business;
- Establish **reasonable policies and procedures** to
  - **IDENTIFY red flags** *relevant* to the bank,
  - **DETECT the red flags** in the course of bank operations,
  - **RESPOND appropriately** to red flags detected (contingency rules), and
  - **UPDATE the program periodically** to account for institutional changes.

Services Offered

The Inquesta Corporation can provide you with a highly-qualified consulting team that can help you be FACT Act compliant.

Our Red Flags Rule projects follow the following trajectory:



A project can span from three weeks to two months, depending on the business' complexity and the number of products/services offered to consumers.

The Inquesta Team

An ITP program's Achilles heel is a poorly constructed set of red flags. More red flags than necessary weaken the institution's focus for true warning signals; and missing red flags will leave the institution vulnerable. This means that to make sound red flag determinations the consultants should be:

- highly sensitized to the criminal mind;
- trained in financial crimes investigation by a federal or state agency;
- experienced investigating white collar crime, particularly crimes that involve stolen identity;
- experienced in regulatory compliance; and be
- accomplished writers (for the creation of manuals and training materials).

These are all attributes that the Inquesta consulting team will bring to your project to implement a robust and defensible Red Flags Rule program for your business.

Once you engage us to comply with the Red Flags Rule, our executives and lead consultants will schedule an experienced project team.