

# Control Essentials

Volume III, Issue III

March 2008

## Identity Theft: New Regulations

### What is Identity Theft?

Fraud that is committed when an individual uses personal information such as the social security number, account number and/or drivers license number of another person without his/her permission.

Identity thieves can obtain access to your bank account and transfer funds to other accounts as well as incur fraudulent charges on credit card accounts. Furthermore, identity thieves can open new accounts in your name, incur expenses and never pay the bills. Such fraudulent actions will negatively affect your credit rating.



### Federal Law: Brief history

In 2003, the United States Congress reacted to the increasing problem of identity theft by amending the Fair Credit Reporting Act with sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act).

### New Regulations

In November of 2007, several Federal agencies issued their joint final rules and guidelines concerning "Identity Theft Red Flags and Address Discrepancies." The agencies include the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), and the Federal Trade Commission (FTC). The joint final rules and guidelines became effective on January 1, 2008. *The mandatory compliance date for these final rules is November 1, 2008.*

### Key Components of New Regulations and Guidelines:

The new rules and guidelines require the following primary components:

- Development, implementation and enforcement of an Identity Theft Prevention Program
- Performance of on-going and comprehensive risk assessments
- Development of specific policies, procedures and practices to combat identity theft issues
- Training for entity personnel
- Oversight of service providers
- Management and oversight of the Program

### IT Security:

Information security design and Implementation  
 Vulnerability Assessments  
 Penetration Testing  
 Security Breach Investigation and Remediation  
 Business Continuity Planning  
 Logwatch  
 Training

### Risk Management:

Risk Assessment  
 IT Risk Advisory  
 Fraud Detection

### Forensic Services:

Computer Forensics  
 E-Discovery

### IT Audit Services:

Application and System Implementation Reviews  
 Internal Information Systems Audits

### Regulatory Compliance:

Bank Secrecy Act  
 Gramm-Leach-Bliley Act  
 Fair and Accurate Credit Transactions Act  
 Sarbanes-Oxley Act  
 Health Insurance Portability and Accountability Act  
 Family Educational Rights and Privacy Act  
 Payment Card Industry

### Attestation Services:

SAS 70 Reviews  
 Other Attestation Services

### **Who should have the Identity Theft Prevention Program?**

Financial institutions and creditors such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, etc that offer or maintain one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing *covered account*.

#### *What is a 'covered account'?*

A 'covered account' is an account used primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account and savings account.

It is also defined as any other account that the financial institutions or creditors offer or maintain for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institutions or creditors from identity theft, including financial, operational, compliance, reputation, or litigation risks.

### **Scope of the Identity Theft Prevention Program**

The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Financial institutions or creditors must perform periodic risk assessments to determine whether they offer or maintain covered accounts

#### **The Program must contain 'reasonable policies, procedures and practices' to:**

*Identify identity theft red flags* (patterns, practices and activities that indicate possible identity theft). When identifying red flags the entity must consider the types of covered accounts it offers and/or maintains; the methods it provides to open its covered accounts; the methods it provides to access its covered accounts, and its previous experiences with identity theft problems.

*Detect identity theft red flags.* Such policies, procedures and practices must cover measures like obtaining and verifying identifying information about the individuals, authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

*Respond to identity theft red flags in a way that is commensurate with the degree of risk posed.* For instance, the practices used to respond to a computer security breach compromising the data of many clients or the compromise of customer data via a fraudulent web site will have to be very different than the ones required to control the compromise of customer data contained on hard copy documents. The prevention and mitigation measures to respond to identity theft red flags should include the use of better logical and physical security measures, on-going monitoring of account activity, closing selective accounts and notifying law enforcement.

*Form a reasonable belief* that a consumer report relates to the consumer about whom it has requested a report, when the entity receives a notice of address discrepancy.

*Provide an address* for the consumer that the entity has reasonably confirmed is accurate to the consumer reporting agency from which it received the notice of address discrepancy.

*Assess the validity of a change of address* if a credit card issuer receives notification of a change of address for a consumer's debit or credit card account and within a short period of time after the card issuer receives a request for an additional or replacement card for the same account.



**Management must approve, oversee and update the program**

The board of directors, an appropriate committee of the board of directors or a designated employee at the level of senior management must formally approve the Program and must be responsible for the oversight, development, implementation and administration of the Program. The board of directors or designated senior management personnel must assign specific responsibility for the Program's implementation, review status reports prepared by entity personnel designated to implement the Program and approve necessary changes to the Program.

The Program must address appropriate and effective oversight of service provider arrangements. Financial institutions or creditors should take steps to ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Financial institutions or creditors should require service providers by contract to have policies and procedures to detect relevant Red Flags as well as report the Red Flags to the financial institutions or creditors.

The Program must address the necessary staff training to effectively implement the Program.

The Program must be updated periodically to reflect changes in risks such as changes in identity theft methods used, entity experience with identity theft problems, and changes in the business structure such as a merger and hiring a new service provider.

**CLIENTS SPEAK FOR ERM**

*They have the ability to understand the needs of our organization and work well with our employees.*

**THE INTERNATIONAL BANK OF MIAMI**

*We selected ERM because of their professional references, experience and reasonable professional fees.*

**R G PREMIER BANK OF PUERTO RICO**

*ERM accomplished and exceeded objectives planned*

**BACARDI - MARTINI, INC.**



## KEEPING WATCH OVER YOUR BEST BUSINESS INTERESTS

**ERM** professionals bring a unique mix of strong academic backgrounds complemented by professional experience ranging from "Big Four" consulting firms to major corporations and prestigious professional certifications. A snapshot of ERM's profile can be seen below:

### Education

#### *Qualifications*

M. S. in Computer Information Systems  
M. S. in Information Networking  
M. S. in Management Information Systems  
Master of Accounting Information Systems  
Master of Business Administration

#### *Universities*

Carnegie Mellon University  
Syracuse University  
Xavier University  
University of Miami  
Florida International University

### Certifications

Certified Public Accountant (CPA)  
Certified Information Systems Security Professional (CISSP)  
Certified Information Systems Auditor (CISA)  
Certified Information Systems Manager (CISM)  
Certified Information Technology Professional (CITP)  
GIAC Security Essentials Certification  
GIAC Systems and Network Auditor  
Microsoft Certified Professional

### Prior Work Experience

PriceWaterhouse Coopers  
Deloitte  
CERT® Coordination Center  
SONY Electronics Latin America, Inc.  
RJR Nabisco  
Diageo plc  
Arthur Young  
Carnegie Mellon CyLab  
Evertec Inc.  
American Bankers Insurance Group  
Chesebrough Pond's  
Starboard Cruise Services, Inc.

### Some of our Clients...

ABN AMRO Private Banking  
Bacardi-Martini, Inc.  
Carnival Cruise Lines  
CitiBank  
Commerce Bank  
Florida Power & Light Company  
Knight Ridder  
North Broward Hospital District  
Ocean Bank  
Rinker Materials  
Sylvania Lighting International  
The International Bank of Miami

**enterprise risk management**

*The Control Professionals*

800 S. Douglas Road, North Tower (# 835),  
Coral Gables, FL 33134.

P: (305) 447 6750 F: (305) 447 6752

Email: [info@emrisk.com](mailto:info@emrisk.com) Web: [www.emrisk.com](http://www.emrisk.com)