LOWERS & ASSOCIATES
International Risk Mitigation Partners
125 East Hirst Road, Suite 3C | Purcellville, VA 20132

Identity Theft Red Flags Rules
Lowers & Associates Program Assistance

The Federal Trade Commission (FTC) and other federally financed regulatory agencies have recently published their final rules and guidelines for regulating the fraudulent attempt to use private information without authority. The new regulations implemented Section 114 (Red Flag Guidelines) and Section 315 (Reconciling Address Discrepancies) of the Fair and Accurate Credit Transaction Act (FACTA). The final rule became effective on January 1, 2008, and requires financial institutions and creditors to develop and implement an Identity Theft Prevention Program for combating identity theft by May 1, 2009. Financial organizations and creditors that do not comply with the requirements risk the threats of fines and/or civil litigation.

Every financial institution or creditor that offers or maintains 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. The Program must involve the Board of Directors or an appropriate committee of the Board, and be updated and approved periodically. In addition, the program must exercise appropriate and effective oversight of service provider arrangements, and train staff to effectively implement the Program. Some 26 examples of Red Flags are described in the final rule.

Lowers & Associates (L&A) assists clients in assessing Identity Theft Program readiness and in the development and implementation of a Prevention Program to achieve a common minimum security level that protects account information. Our services include the following:

- Data Flow Analysis: L&A indentifies all devices, systems, and applications that process or store account data, and is critical to designing appropriate remediation steps for any gaps identified.
- Preliminary Gap Analysis: L&A identifies all appropriate controls in place, so as to carefully compare the processing environment to the Identity Theft Red Flags Rule requirements, highlighting any gaps and vulnerabilities which might exist.
- Risk Assessment: We then conduct a Security Risk Assessment that focuses on protecting information assets from known vulnerabilities and typical threats.
- Identity Theft Prevention Program Development: L&A concludes the effort by putting in place appropriate policies and procedures and by defining and documenting the program for third-party review.

Financial institutions and creditors faced with this compliance requirement need to be proactive and initiate a plan to build an Identity Theft Prevention Program. L&A can assist in positioning Identity Theft controls across the organization, therefore enhancing the overall security posture and reducing the likelihood of unauthorized individuals gaining access to sensitive information.