



October 8, 2008

Secure Identity Systems Helps Springfield State Bank Comply with Red Flag Regulations

Business Wire - Press Release

Springfield State Bank, a locally owned and operated bank serving Washington County, Ky., has signed Secure Identity Systems to help the bank move towards Red Flag compliance in time for the FTC's Nov. 1 deadline. As part of this, SIS will conduct an Initial Risk Assessment, develop a customized Policies & Procedures Manual, and provide New Account Authentication and Change of Address Verification for all consumer accounts.

"Secure Identity Systems offers comprehensive services that specifically meet the requirements for Red Flag compliance," says Robbie Polin, CEO for Springfield State Bank. "We knew they were the company who could properly evaluate and improve our current identity protection programs, protect our customers from the threat of identity fraud, and move our institution into alignment with the FTC's regulations."

Section 114 of the FACT Act requires all banks and financial institutions to formally address the risks of identity theft, and develop and implement identity theft protection procedures to mitigate those risks.

With the Initial Risk Assessment and Policies and Procedures Manual, Secure Identity Systems will evaluate Springfield State Bank's current identity protection strategies, as well as Bank Secrecy Act (BSA) requirements, information security, and identity theft risk factors. They also will outline the measures the bank must implement to detect, prevent, and mitigate fraud.

Secure Identity Systems' New Account Authentication will help Springfield State Bank take authentication beyond the standard two forms of ID. When a customer attempts to open a new account, SIS's solution instantly consults a series of databases, including the Social Security Administration, credit bureaus, and local property databases, for the most accurate and current information to authenticate the identity of the new account holder. SIS also provides USA Patriot Act compliance, checking customer ID information against OFAC and multiple other government watch lists.

Similarly, each time a customer requests to change the address on an existing consumer account, SIS's Change of Address Verification solution searches a database of more than 700 million records and identifies the level of risk associated with the address change in mere seconds. Banks using this solution are able to verify approximately 25 percent more potential threats, virtually eliminating the chance a fraudster can alter an address and hijack a consumer account.

"According to a recent study by Unisys, 50 percent of consumers indicated that they would switch their financial institution for one that offered better protection against ID theft," says Bryan Ansley, CEO of Secure Identity Systems. "These protections are about more than just meeting regulation requirements. They are critical for financial institutions to retain customers, maintain customer loyalty, and provide a better banking experience. We are dedicated to working with banks like Springfield State to assist them in these tasks and offer the solutions to meet the needs of the government regulators and consumers."

Secure Identity Systems is the only company in the United States to offer financial institutions a complete, end-to-end solution for Red Flag compliance. For more information about Secure Identity Systems' array of ID fraud protection services, including New Account Authentication, Anti-phishing Detection and Take-down, and mConfirm Authentication, visit www.SecureIdentitySystems.com.

ABOUT SECURE IDENTITY SYSTEMS

Secure Identity Systems is the leading provider of fully managed, total identity theft protection systems that safeguard financial institutions, businesses, individuals, and households. For more information, visit www.SecureIdentitySystems.com. annual self-assessment questionnaire.