FOR IMMEDIATE RELEASE

Contact: Paul Tomasofsky
(201) 775- 4960
PaulT@SecureRemotePaymentCouncil.org

SECURE REMOTE PAYMENT COUNCIL PUBLISHES FOURTH POSITION PAPER IN SERIES ON TRANSACTION SECURITY

Westwood, NJ – December 3, 2015 – The Secure Remote Payment Council (SRPc) has just released its fourth position paper in a series on transaction security, this time wrestling with preventative measures to combat identity theft.

As its victims will attest, identity theft can be the result of fraud perpetrated on an existing payment card account. With the growing amount of personally identifiable information readily available on the Internet, Merchants and Financial Institutions are looking for safe and secure identity management solutions to protect their clients - and with good reason. According to the Identity Theft Resource Center, a not-for-profit organization that assists consumers with identity theft, 38.9 percent of consumers changed their bank, credit union, or credit card company when unauthorized activity occurs on their existing account.

The SRPc Authentication Work Group posits that out-of-band, multi-factor authentication provides the best defense against Internet and point-of-sale fraud. They address the barriers to entry in the deployment of user authentication solutions and the misperceptions in the marketplace that have hampered widespread adoption.

Consumer acceptance is an imperative. “Authentication techniques must be easy for the consumer to use and must provide a high degree of protection against misuse of personally identifiable information (PII),” said Paul Tomasofsky, president and executive director of the Secure Remote Payment Council. “The experience for the consumer must be frictionless. If the enrollment process is onerous, authentication adoption will never become widespread,” he added.

The Work Group endorses risk based identity verification that factors the dollar amount of the transaction while gauging the level of confidence required to determine if the transaction is good. They also noted that the value of what is being protected must be greater than the cost of protecting it.

In the Call to Action, the SRPc Work Group strongly recommends a number of guiding principles for user authentication which include the endorsement of a multi-layered approach for security, interoperability among the stakeholders across all delivery channels, and a balanced governance structure for the assignation of liability. These are common themes expressed by the Work Group about transaction security in general, but no less relevant in this specific application.

The SRPc Authentication Work Group’s mission is to collect, evaluate and comment upon common ideas, statements and positions promulgated in the payments industry related to transaction security. The Work Group is a team comprised of payment experts representing a broad cross-section of industry stakeholders. For more about the SRPc and to see the position paper visit: http://www.SecureRemotePaymentCouncil.org