

**Byron F. Bowman**  
Direct Phone: 412.288.1963  
Email: [bbowman@reedsmith.com](mailto:bbowman@reedsmith.com)

Reed Smith LLP  
Federated Investors Tower  
12th Floor  
1001 Liberty Avenue  
Pittsburgh, PA 15222-3779  
412.288.3131  
Fax 412.288.3063

July 13, 2006

Advisor Security Inc.  
2323 High Mountain Drive  
Salt Lake City, Utah 84092

Re: Data Protection Responsibilities of Brokers for Remote Advisors

You have asked us for our advice on the legal and regulatory responsibilities of independent broker-dealer firms for data protection in a distributed communications environment. Specifically, you asked us to comment on a broker's responsibilities for data protection when its registered representatives ("advisors") operate from independent remote offices and with their own personal computers. We have concluded that, in addition to the litigation risk faced by all businesses with respect to data security, independent broker-dealers face industry-specific risks and obligations. Moreover, the number, complexity, and severity of these risks and obligations have increased sharply in recent years, driven by public concerns over identity theft and institutional commitment to data security issues by regulators. As standards for data security continue to ratchet up, specific action by the independent broker-dealers and their advisors to address the added level of risk seems advisable. To make the transition from nominal policy to on-the-ground reality, and to provide evidence of compliance useful for defending litigation which may arise subsequent to any breach, each of the steps discussed herein should be not only implemented but systematically documented, audited, and verified.

### *Introduction: Data Security Breaches, Remote Work, and the Human Element*

Participants in the financial industry have been hit hard with very public data security breaches of late, with resultant bad publicity, loss of consumer goodwill, and exposure to regulatory action or class action suit. In June of this year, AIG announced that a burglar at its corporate offices had stolen a company server, and that the server contained the names, Social Security numbers, and in many cases

medical information of almost a million people. But in many cases the loss of customer information, either in electronic or paper form, occurs outside the better-protected confines of the central workplace. The Fidelity Investments breach, which involved personal information on almost 200,000 retirement account customers, occurred when Fidelity employees took a laptop on a routine business meeting. The laptop was stolen, along with all the sensitive personal information on it. In late December of last year, an Ameriprise employee left a laptop in his car. The laptop contained names, Social Security numbers, and Ameriprise account information on an “unknown” number of customers, estimated at over 230,000. This laptop was also stolen. The AIG, Fidelity, and Ameriprise incidents are just three recent cases where exposure of customer information made the papers; three incidents out of hundreds reported in the last two years. In many reported incidents of breach, the breaching firm had clear guidelines prohibiting employees or vendors from taking unencrypted personal information about customers outside the office. Apparently, as identified in the survey of field practices you have conducted and which is attached as an Exhibit hereto, such well-meaning and well-drafted policies are very often ignored and violated.

More than any other element in data security, the human element risks failure in the absence of dedicated, comprehensive, and sustained oversight to achieve a compliance orientation. The corporate tendency to pigeonhole data security as an IT problem to be dealt with by IT staff has ignored the sizeable non-technical aspects of the problem. These include workplace training; processes for the creation, storage, daily management, secure retention, and destruction of hard copy files; supervision of office, telecommuting, and remote access practices; and rigorous management of access profiles. Failure to think comprehensively about data security, both inside and outside the physical office, has cost companies dearly.

### ***Data Security Risks Specific to the Independent Broker-Dealer Context***

Typically, independent broker-dealers have concentrated their data protection efforts on their own primary network, implementing safeguards such as secure transaction platforms, firewalls, secure e-mail, and limitations on instant messaging. However, as personal computing technology has developed, there is an increasing tendency for affiliated independent advisors and their employees to use their personal computers to establish remote access with the independent broker-dealer’s primary system and to engage in a substantial amount of work at remote locations. Advisors themselves store and share large amounts of customer information, in both paper and electronic form. To comply with legal requirements and to effectively provide investment services, such widespread custodianship of customer information is inevitable. These remote locations from which advisors work, be they offices, homes, or