

CU SECURITY - ESTABLISHING A PROACTIVE APPROACH

The traditional security principles are pretty well known: facilities, personnel, documentation, systems, data, and communications. Now we have to add consideration for both fraud risks and Patriot Act compliance. Each one of these has its own issues and solutions and in many cases there are complex overlapping questions. Since each credit union is a unique proposition with respect to its market location and competition, membership, products and services, physical and systems plant, it can be a very difficult task to get all of the pieces to fit together in a coherent, reasonable and affordable security program.

The problem with hackers/crackers is that they seek paths of least resistance and have the ability to screen across the whole range of opportunities for attack. My suspicions are that the smaller the organization the more vulnerable it probably is. On the other hand, every CU has to maintain awareness of the potential for insider threats. Most internal fraud and abuse cases occur after some life changing experience to an employee (e.g., divorce, debt, illness, etc.). It's important to note that only about 3% of the fraud cases are discovered by internal auditors. So there needs to be a system of supervisory awareness of employee behavior that suggests internal fraud.

Our solutions focus on preventing fraud and abuse, as well as satisfying the compliance requirements of the U.S. Patriot Acts. Currently three systems are available for new member identity screening, account activity analysis, and bad check (closed account) detection. The backbone system, RiskTracker™, currently has the ability to detect well over 30 Billion different combinations of risk for a single transaction. RiskTracker™ is provided as a service to our clients, so it is continually upgraded through the continual feedback we get from our clients. The entire focus of our business is on prevention, since once a fraud loss occurs it is infrequent that the funds are ever recovered by traditional investigation and collection means.

All of our systems are installed in the credit union and are operated by credit union employees. Because the systems are comprehensive and easy to understand, employees gain in their knowledge of the threats and prevention methods. Since the systems maintain a formal record of daily risk management efforts and results, they provide a detailed means to demonstrate to auditors how loss prevention and compliance programs are working.

Risk management and particularly fraud, money laundering and terrorism financing are complex issues. While our systems and services are constantly upgraded as the threat changes, the real foundation of knowledge is provided by our clients as part of a networked community with common goals. It is this feedback that gives us the guidance and priority for new analytical methods and products. Without this broad base of knowledge, our technology would become static and out of date.



Robert Cofod is the President and CEO of FRAUDetect, L.L.C. During his twenty-five year career in military and national intelligence organizations he was either responsible for or a participant in the design and development of well over thirty advanced intelligence collection and analysis systems. During this time he focused on numerous intelligence problems that were rooted in either deception or counter-deception - practices that are closely related to fraud. In 1996, Mr. Cofod developed a new account bank fraud product for Riggs National Bank. From that initial effort he has continued to lead the development of several additional products aimed at the prevention of fraud and abuse. FRAUDetect currently provides advanced fraud and abuse prevention products and services to financial institutions worldwide.