The Problem
Fraud and deception pervade almost every aspect of modern life. Existing automated tools for detecting or deterring fraud often fall short. They rely mainly on historical information and can only flag malicious activity after it has occurred. Many such systems are plagued by high false positive rates, making follow-up investigations extremely inefficient, expensive, and nearly impossible to make comprehensive. Approaches that dive into additional nuanced detail, such as the polygraph, are not scalable - they are expensive and time consuming to deploy.

Our Approach
In order to improve fraud detection and deterrence, we take an approach that generates additional information about the state of mind or intent of the user. This new information can then be used to improve the classification of actors as potentially malicious or not. We flag potentially suspicious answers to questions in online forms designed to elicit risk-relevant answers. Flagged users can then be subjected to additional follow-up procedures or investigation as appropriate.

The Science
Deceptive intent on the part of an actor is hard to measure directly. Intent manifests itself as an internal mental state. These mental states are also hard to measure, requiring large equipment such as fMRI machines. Fortunately, psychology research has show that the mental states associated with deception and malicious intent lead to uncontrolled physiological changes such as emotional arousal and cognitive conflict.

Recent neuroscience research has shown that these emotional and cognitive states have an immediate and uncontrollable impact on the motor nervous system, the part of the nervous system that controls our movements. Computer interface devices, such as mice and touch screens, are effectively highly precise sensors that can be used to measure the movements of the human body.

Our research has shown that we can use these interface devices to generate measurable signals that are associated with malicious or deceptive intent. We then combine these signals using patented algorithms to identify suspicious behavior and potentially deceptive responses.

The Technology
Our technology utilizes commonly available input devices, such as keyboards, mice, touch screens, and mobile devices, to capture motor nervous system signals. We analyze these signals to identify movement patterns associated with deceptive behavior or intent. We then use our patented algorithms to identify suspicious behavior and potentially deceptive responses. Our technology is:

Scalable: Our software is designed using industry standards for cloud based architecture. This allows for easy and exceptional scalability. We can handle millions of simultaneous users. In addition, our platform can be hosted on both public and private cloud systems, allowing for a very high level of security.

Deployable: No special hardware is required; we use commonly available input devices, such as mice and mobile devices, to capture motor nervous system signals. Our software integrates with existing HTML-based forms using a simple JavaScript library and has a minimal impact on existing processes and systems.

Customized: Additional information about the intent of potentially malicious actors is only useful if it is relevant to the risk at hand. Our professionals have extensive experience in the psychology of malicious activity. We use this background to help build questionnaires that are tailored to the risks you face.

About Neuro-ID
Neuro-ID, Inc. is a science and software company that provides a scalable platform for the detection of suspicious behavior that is indicative of fraud and other online threats. Our clients gain information about user behavior and intent, allowing faster and better decision making to better manage risk and investigative resources. We serve the insurance, financial services, healthcare, public sector, and other industries.

Our patented technology was invented at the University of Arizona and Brigham Young University and is exclusively licensed to Neuro-ID.

For more information: www.neuro-id.com

Copyright © 2016 Neuro-ID, Inc.