

# DeviceInsight™

## Intelligent Fraud Identification for Financial Services Online

In the criminal world, anonymity is a vital asset. Bank robbers don't present their drivers' licenses when they hold up a bank. They disguise themselves with a stocking or a Halloween mask. But on the Internet, anonymity is built in. There is no way to know with certainty who is actually conducting a transaction. This, combined with the fact that the Internet enables any target to be "attacked" from anywhere in the world at any time, frames the challenge for Internet fraud management.

### Inadequate Protections Against a Growing Threat

Several technologies have evolved over the last decade in response. Credentialing systems seek to establish ever stronger authentication. But customer adoption, lack of standardization and expense remain significant barriers to broad deployment. In addition, transaction monitoring systems utilizing sophisticated pattern recognition technologies can detect fraudulent behaviors after the fact. However, these are expensive to implement and generate high rates of false positives.

IP Address resolution looked to be a promising method to distinguish customers from fraudsters, but IP "spoofing" has limited its effectiveness. Regulatory guidance in the financial services sector has driven an increase in the deployment of device tagging, such as cookies, to authenticate a device in combination with a user-entered credential (such as username/password). But criminals now steal the cookies, along with user credentials, leaving consumers no safer.

### The New Standard in Fraud Detection

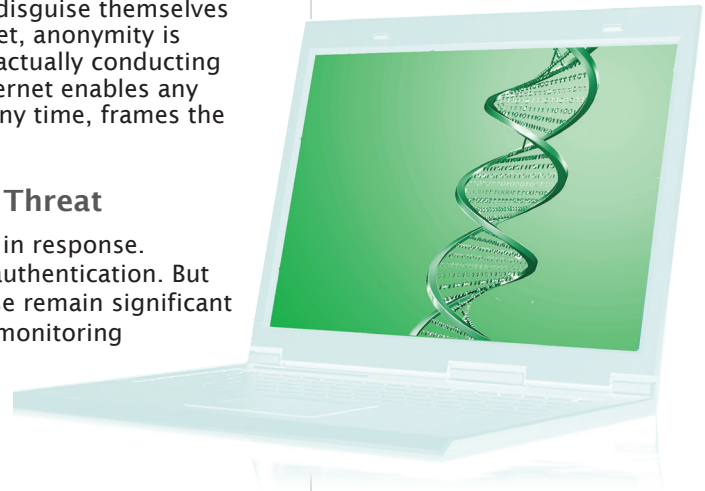
Enter **DeviceInsight** from 41st Parameter. Requiring no user involvement, hardware deployment or disruption to the user experience, **DeviceInsight** enables financial services sites to "converse" with transacting devices. Through this non-obtrusive, automatically conducted conversation, a digital fingerprint for the device is created, which can be used to match devices to log-ins or transactions.

### Easily Integrate Your Fraud Fighting Efforts

Specific information gathered from the device can also be used to identify downstream risk or perform analytic applications. **DeviceInsight** operates in real time and can be easily integrated into any webpage to reduce the anonymity of the transactor. In effect, **DeviceInsight** is the difference between assuming that your users are on the other end, and knowing they are.

As one of the few technologies that enable an institution to link abuse in one channel to the potential for abuse in another, **DeviceInsight** is especially useful in companies who are managing a variety of applications online. For example, a retail banking operation could share information on abusive devices with the small business or corporate bank team, even though the respective applications are totally segregated.

41st Parameter utilizes **DeviceInsight** in its risk management and authentication applications directly. However, the open API of **DeviceInsight** allows it to be easily integrated into existing, custom developed applications. Operating with any device connecting to the website, including mobile devices and game consoles, through any browser connection, **DeviceInsight** affords the flexibility to provide content access the way customers desire it. Enhancing the effectiveness of existing systems and enabling improved analysis to support superior risk management for the on-line channel is a primary goal of all 41st Parameter technologies.



Make secure instant decisions such as on-line credit

Authenticate based on whether the device is "known" to the account

Detect compromised accounts by evaluating if one device is using credentials of many individuals

Identify account abuse, such as violation of usage agreements for digital content account takeover, based on an "unknown" device executing a transaction within an account