RISKY BUSINESS

Using business intelligence technologies to spot high-risk transactions, authenticate customer identities, and prevent fraud helps keep your operation running in high gear.

It's a simple fact: money attracts crime. And in a world where the bulk of worldwide transactions occur through electronic systems, it can be even easier for perpetrators to slip under the radar and commit fraud or launder funds without anyone noticing. All too often, enterprises don't discover that illegal or fraudulent transactions have taken place until it's too late to do anything about it.

In addition, fraud and money laundering can expose enterprises to hefty regulatory compliance fines and cause significant damage to shareholder trust, which presents executives with a thorny problem: as criminals have escalated their level of sophistication, fraud challenges have become increasingly subtle and difficult to detect. At the same time, traditional data management and analysis approaches are limited in their ability to identify and respond to these attacks.

> **"All too often, enterprises don't discover that illegal or fraudulent transactions have taken place until it's too late to do anything about it."**

Combating potential threats by using information effectively is more important than ever for several key reasons:

- **Threat variety has increased.** In the past decade, enterprises have encountered many new types of threats as criminals have become more sophisticated.
- **Threats have become increasingly asymmetric.** In the past, perpetrators generally needed to have money and a certain level of organization and expertise to cause significant damage—but today, a relatively unsophisticated criminal with some imagination and a good laptop can cause major damage.
- **Threat identification has become more complex.** Fraudsters and money launderers are simply getting better at what they do. Many attempt to hide who they really are to avoid suspicion until it is too late to prevent the fraud. For example, criminal and terror syndicates are increasingly using shell companies and fronts that appear to be legitimate businesses.
- **Globalization has pushed threat activity across national boundaries.** Since 9/11, the threat and fraud challenges organizations are facing have increasingly cut across geographic and cultural lines.
- **Regulatory and stockholder pressures have intensified.** Enterprises face strict compliance requirements regarding customer identification—and, to compound the problem, shareholders who have seen their stock prices tumble are unlikely to forgive oversights that leave the organization exposed to both governmental fines and embarrassment in the press.

Leaders in a variety of industries have responded to these trends by pushing for an active, dynamic threat and fraud intelligence capability that allows them to identify and prevent attacks and crime—accurately and in real time. But although many executives embrace this concept in theory, the best way to execute the vision of a dynamic threat prevention system is not always clear. Companies can take a broad range of approaches, from pattern and

behavioral analysis to identity authentication and data mining. With limited budgetary resources, though, the real question is one of priority. Where should enterprise IT departments invest to get the most tactical benefit while also positioning for long-term competitive advantage and return on investment?

The answer: business intelligence. Meeting the challenges of fraud and money laundering requires the real-time operational detection and prevention that business intelligence solutions are designed to provide, offering a powerful weapon against these complex threats.

"Business intelligence works to combat fraud by bringing together data that resides in multiple systems throughout the enterprise to create a single comprehensive picture of the best information available."

Business intelligence technologies are critical to helping companies spot fraud, because they provide the key to understanding identity. In an increasingly complex and international society, identities can be easily blurred. Fraud perpetrators often try to evade investigators by hiding or masking their identities—which is why it is critical to understand who your customers truly are. Because business intelligence solutions bring together data from multiple siloed systems across the enterprise, they can help automate the flagging of potentially suspicious duplications and inconsistencies in customer records. They can also help companies uncover relationships between potentially suspicious customers, as well as patterns of behavior that may signal money laundering activity.

Natural processes are constantly at work to degrade information, and silos of information exist across virtually every enterprise. Organizations merge and combine databases. New accounts and cases are constantly open and closed. People get married, separated, and divorced. Letters are inadvertently transposed. All of these events can cause information to degrade or drift. For these reasons, business intelligence modules that are designed to cleanse and repair data also contribute to the struggle against fraudulent and criminal activity.

In a perfect world, this data degradation would be the only force blurring customer identities. But perpetrators also frequently take advantage of cultural ambiguities and compound the problem by intentionally misrepresenting their identities—which makes maintaining an accurate view much more difficult.

Business intelligence works to combat fraud by bringing together data that resides in multiple systems throughout the enterprise to create a single comprehensive picture of the best information available. By increasing the transparency of business operations in this manner, your enterprise can more easily perform auditing functions to help spot potentially suspicious activity. But no matter how transparent operations are, the sheer volume of customer activity data you collect puts effective auditing by human beings beyond the realm of feasibility. That's where business intelligence technologies excel: through automation, they can comb through hundreds of thousands of transactions in near real time to reveal patterns that may indicate fraudulent activity.

However, using business intelligence technologies for combating fraud and money laundering is not a magic bullet. Even the most sophisticated, high-performance business intelligence solution cannot interpret the pattern of anomalies it reveals. Once inconsistent behaviors or discrepancies among records are detected, it is up to the professionals in your enterprise to decide what is suspicious and what is not—as well as what to do about it.

As threat variety and complexity have increased, the ability to fight fraud and money laundering through effective use of information has become increasingly critical. Business intelligence solutions are a key tool in this ongoing battle. By aggregating data from systems across the enterprise and using it to synthesize actionable information, business intelligence technologies can arm enterprises with a new and extremely powerful weapon in their fight against fraud and money laundering.