Deloitte.

Risk Angles
Five questions on financial crime

An interview with Peter Dent, Deloitte Canada partner and leader of its Forensic services practice and Global Financial Crime Initiative, and closer look by Anthony DeSantis, principal in the Data Analytics practice within Deloitte Transactions and Business Analytics LLP, an affiliate of Deloitte Financial Advisory Services LLP in the United States.

Financial crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and revenue of many organizations. In addition to the risk of losses from financial crime itself, companies also face spiraling costs in related areas. Compliance with increasing regulation, ongoing crime detection efforts, internal investigations of potential wrongdoing, external enforcement actions and any associated fines and penalties, class action lawsuits, and other litigation are among the factors driving up both the costs and risks associated with financial crime. In order to effectively detect, assess, prevent, and respond to financial crime, organizations should consider a more strategic and holistic risk management approach.

In this issue of Risk Angles, Peter Dent answers five questions about managing the risks of financial crime, and Anthony DeSantis discusses the use of Big Data to proactively address fraud risk.

Question	Peter's take
What do we mean by financial crime?	From fraud to electronic crime, from money laundering to bribery and corruption, from market abuse and insider dealing to sanctions — all of these forms of financial crime are on the rise and share a common denominator: money.
Why does financial crime pose a bigger threat today?	Financial crime is an ever-present threat for organizations. The value of what criminals actually take is only part of the cost – there are also penalties, civil judgments, and the cost of litigation and conducting investigations. Corporate officers may feel a perfect storm of pressure. Bribery, fraud, and cybercrime keep getting more sophisticated. Regulatory agencies demand more accountability and as business embraces globalization, it encounters nuanced new cultural and legal challenges.
How are companies managing the risks associated with financial crime?	A fragmented approach isn't enough and neither is a purely reactive one. Compliance-based approaches addressing particular risks in a siloed or piecemeal fashion are giving way to holistic approaches that look at many types of financial crime risk across the organization. Regulators expect to see this risk-based approach, yet still expect an overall compliance strategy. Regulators are looking for someone such as a Chief Compliance Officer or Chief Legal Officer to have over-arching responsibility. Overall, the trend is toward a broader risk-based approach with shared responsibility by management, staff, the board of directors, and internal audit. Accomplishing this transition typically involves a focused change management effort for the organization.
Why do companies' compliance, anti-fraud, anti-money laundering, and similar programs fail?	Failure to prevent or detect issues is often not because the programs or controls themselves are lacking. More often, it's a failure of culture and a lack of effective change management. For example, senior leaders may not be setting a strong or consistent "tone at the top" about acceptable and unacceptable behaviors. Or perhaps there isn't enough attention paid to gaining buy-in from the lines of business for new policies or processes. Or staff training and awareness efforts may be lacking. The infrastructure to prevent financial crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time — culture is what enables and drives those appropriate behaviors.
What role does technology play in managing financial crime risk?	Technology tools can give organizations a more holistic view of their data, highlight potential areas of risk and allow them to be more focused or targeted in their efforts to combat financial crime. Advanced analytics may help companies be more predictive in identifying trends and patterns indicative of financial crime risk that are not otherwise easily discernable. Overall, the emphasis today is on prevention and/or early detection; leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news.

A closer look: Big Data's role in fighting financial crime

By Anthony DeSantis

"Big Data" has become a commonly used term to describe the explosion in the volume, variety, and speed of information generated in the course of our daily lives. Big Data encompasses:

- **Traditional enterprise data** from customer information systems, ERP data, online transactions, financial data (general ledger, accounts payable, accounts receivable), and the like.
- **Machine- or sensor-generated data** from sources such as Call Detail Records (CDR), weblogs, smart meters, manufacturing sensors, equipment logs, and trading system data.
- **Social data** from customer feedback streams, blogging sites, and social media platforms.

Over the last 10 to 15 years, there has been a leap in the use of data analytics to mine Big Data to identify the patterns, trends, and anomalies that are often indicators of fraud or other types of financial crime. In the past, these have been siloed efforts in response to particular incidents or investigations. Now there appears to be a much broader effort to proactively detect, deter and prevent financial crimes. Big data and analytics are shaping how companies approach these efforts. For example, Enterprise Fraud and Misuse Management (EFM), is becoming more widespread as it allows organizations to integrate technology platforms, methodologies, and analytics approaches to proactively identify the indicators of fraud. EFM can provide a holistic, real-time or near real-time view of data to expose fraud risk across the organization.

As an example, a US federal agency was faced with processing and analyzing massive amounts of structured and unstructured data to continue its oversight and monitoring functions. Implementing an EFM infrastructure allowed it to explore the data efficiently, develop models, and then refine those models to predict and provide alerts about potential fraudulent behavior. Case management was incorporated to manage alerts to resolution, and then those results were fed back into the models to identify positives and false positives in order to improve the models' effectiveness. Social network analysis was utilized to identify previously unknown relationships and expand the network of potentially fraudulent actors and activity.

Even with the advances in technology, many companies simply are trying to figure out where to start. They may be struggling with the amount of data and the daunting task of integrating and condensing it into manageable chunks. Deciding what to focus on and who should own the process are further sticking points. In many instances, it's helpful to take a pilot approach — choosing a particular type of financial crime risk (corruption, for example) or concentrating on a particular region. This can allow you to practice and refine data analysis techniques and methodologies — and see incremental progress — before implementing them on a broader scale.

For more information, contact:

Peter Dent
Global Financial Crime Initiative Leader
Deloitte Canada
+1 416 601 6692
pdent@deloitte.ca

Anthony DeSantis
Principal
Deloitte Financial Advisory Services LLP
+1 212 436 3307
andesantis@deloitte.com

Henry Ristuccia
Global Governance, Risk and Compliance Leader
Deloitte Touche Tohmatsu Limited
+1 212 436 4244
hristuccia@deloitte.com