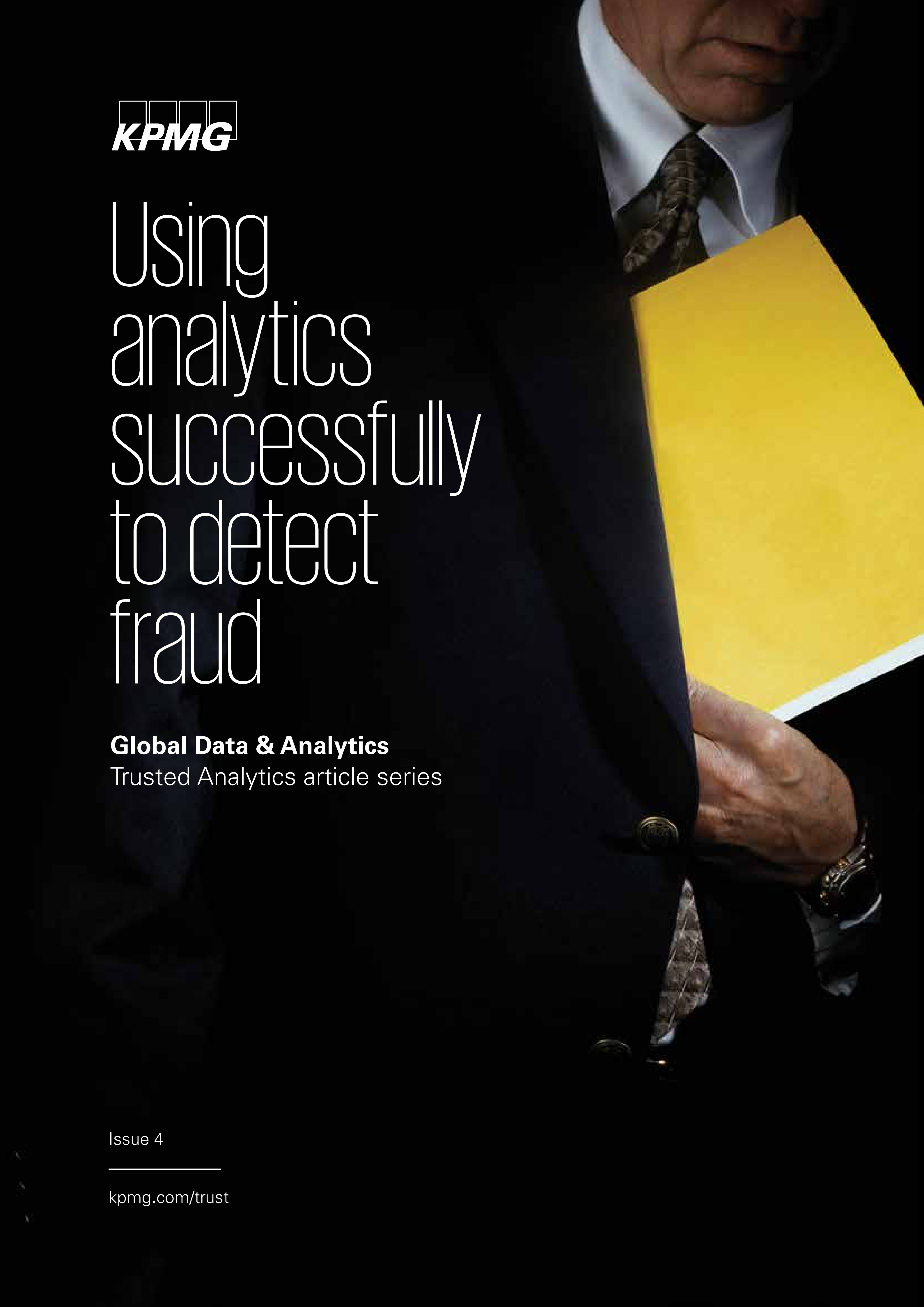

# Using analytics successfully to detect fraud

**Global Data & Analytics**
Trusted Analytics article series

Issue 4

kpmg.com/trust

# Introduction

Trust is the glue that holds society together and makes commerce possible. It permeates business life and touches every aspect of corporate behavior, even in the area of fraud and wrongdoing. People who defraud companies by misappropriating funds or creating false invoices or transactions are abusing a position of trust, whether it's within the company or between the company and outsiders, such as vendors, customers or business partners.

Companies that seek to detect fraud often deploy data and analytics (D&A) to search for anomalous or suspicious transactions. If a detection program is going to succeed, it must have access to reliable data and be trusted to perform according to the company's expectations. Executives must have confidence the analytics will work as intended. D&A can also be used to monitor the behavior and conduct of employees and third parties. This program, too, has to be trusted to be effective.

However, these are not easy objectives to achieve. Confidence in anti-fraud analytics can evaporate quickly if the process is not managed effectively. Getting it wrong can be worse than doing nothing at all, which is perhaps why many companies may be reluctant to deploy analytics programs. In fact, according to recent research by KPMG, very few companies are employing analytics successfully for the detection of fraud. Based on a global survey of KPMG professionals who investigated 750 fraudsters between March 2013 and August 2015, only 3 percent were detected using proactive, fraud-focused analytics, compared with 44 percent who were found by means of whistle-blower mechanisms and other forms of tip-off.[1]

In this latest article in the *Trusted Analytics* series, we examine some of the possible factors behind the low detection rate using analytics and the ways in which companies can build greater confidence and trust in the use of analytics to combat fraud.

Based on our experience in the field, we find that companies face significant issues in how they build and deploy trusted analytics against fraud. If an analytics-driven anti-fraud program does not successfully detect cases of wrongdoing in the early phases, management's confidence in analytics as a valuable tool to pinpoint fraudulent activity could well erode. In this article, we explore the four trust dimensions or anchors to help companies manage trust in an analytics-driven fraud detection program.

> "If an analytics-driven anti-fraud program does not successfully detect cases of wrongdoing in the early phases, management's confidence in analytics as a valuable tool to pinpoint fraudulent activity could well erode."
>
> **Phil Ostwalt**
> Global Investigations Network Leader
> Partner, KPMG in the US

**Phillip Ostwalt**
Global Investigations Network Leader Partner, KPMG in the US

**Gerben Schreurs**
Global Head Forensic Technology
Partner, KPMG in Switzerland

---

[1] Global Profiles of the Fraudster, KPMG International, 2016.

# Why the low usage of such a powerful tool?

The low usage of analytics is a matter of concern because analytics can be an indispensable tool in the highly complex world of fraud detection. This is especially important considering the huge cost of fraud. For example, a 2016 global survey of over 40,000 certified fraud examiners revealed that fraud accounted for US$6.3 billion in losses, with the typical organization losing 5 percent of its revenues annually to fraud.[2]

Why are larger numbers of companies not employing analytics successfully to catch fraudsters? Some corporate decision makers do not understand what analytics can do for them. Others balk at the expense. Still others may believe that until a major fraud occurs at their company, it is not worth the cost of investing in advanced analytics to detect potential wrongdoing before it occurs.

We believe that this lack of adoption also reflects a 'trust deficit' — a lack of trust and confidence that the underlying data, the analysis and the business interpretation of the outcomes will be able to distinguish between legitimate transactions and fraudulent activity in an efficient and cost- effective manner. In other words, there is a general lack of trust in the processes for detecting those employees and business partners who are not 'trustworthy'.

If these trust issues are carefully managed, analytics can be a highly effective addition to any company's anti-fraud program, helping limit potential financial and reputational losses from fraud and misconduct and sending a message to would-be fraudsters that the risk of getting caught may be too high. This is why trusted analytics is an important tool in helping to mitigate security and reputation risk. KPMG's first article in the Trusted Analytics series, *The Power of Trust in Analytics*, explains that trusted analytics is based on four trust dimensions or anchors. Creating a trusted analytics program to monitor and detect fraud is best seen from the same perspective, as we discuss below.

# Successful analytics requires high-quality components

The first trust anchor relates to the **quality** of the components in the analytics program.

Which data to analyze should be directly related to detecting suspicious or questionable transactions or anomalies in the routines, including those that may be indicative of fraud. Therefore, the sources of data for analysis should include the processes in which an employee could possibly influence a transaction, such as employee expense reports, accounts payable and any transaction that includes the handling of cash. The data has to be accurate and up-to-date. The sources of the data need to be known and understood.

It has to be consistent and complete. The program's design should fit the task at hand and be modeled on the processes that are relevant, such as the types of transactions, the involvement of particular functions and so on. These considerations hold true for all types of analytics, including its use to detect fraud, mostly in the form of deliberately falsified information.

---

[2] 2016 Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners (ACFE).

# A critital step: knowing what is normal

Given the vast amount of data generated today, it is natural to think analytics can be of help in detecting fraud. The premise of most anomaly detection methods, even the new ones associated with machine learning, is to identify odd patterns in an otherwise homogeneous population. However, the success of these analytical techniques, especially if fraud is rare, depends on the ability to know what is normal. A successful fraud detection program through analytics must consider detecting both anomalies and knowing what is normal. When analytics-based fraud detection programs fail, it is often not because they lack analytical rigor but because the implementation platform lacks the knowledge of what is expected to be normal. It is much easier to eliminate the honest people, who tend to be more transparent, than to find those who commit fraud. This is akin to lowering the water level of a muddy river to be able to more clearly see the rocks at the bottom, a philosophy used effectively in lean manufacturing systems.

# False positives must be carefully managed

The second trust anchor refers to the **effective use** of the process for analyzing transactions. Is the output accurate and useful in the sense of fulfilling its purpose? A successful anti-fraud analytics process has to walk a fine line between generating too many and too few red flags. Refining the algorithm to achieve this balance is a process of trial and error.

This is an example of engendering trust between the algorithm and the human. In a large, complex organization, it could take several months to achieve an optimal rate of fraud alerts. Careful calibration takes time and organizations must be patient. Data analysts must therefore manage expectations, because decision makers tend to become frustrated if the desired results are not achieved quickly or easily. A wave of euphoria about the effectiveness of the program can easily give way to deep pessimism.

Too many false positives and it might cause corporate leaders, as we mentioned earlier, to lose confidence in the process. If each potential case is investigated aggressively, employees and other stakeholders could also lose faith in the program and trust in their employer.

If there are too few red flags and, as a result, cases of fraud escape detection, this is equally harmful, if not more so. Executives will begin to doubt the effectiveness of the process and seek other methods to meet their objectives. On balance, it may be better to stray on the side of detecting too many false positives. This is because it can sometimes be comforting to know that the company is being vigilant, even if the anomaly investigated does not ultimately lead anywhere. This may actually build trust, not erode it.

> “A successful anti-fraud analytics process has to walk a fine line between generating too many and too few red flags. Refining the algorithm to achieve this balance is a process of trial and error.”
>
> **Gerben Schreurs**
> Global Head Forensic Technology
> Partner, KPMG in Switzerland

## Operational control must be sustainable

Based on our experience in the field, more companies are deploying data analytics for fraud detection. Yet, as we noted earlier, the global survey of fraudsters found that only 3 percent of successful detections used analytics. One reason for the gap is that the long-term **operational control** (trust anchor no. 3) of the analytics processes may not have been established, let alone optimized, with the result that the detection rate is less than expected. While it requires a high level of expertise and technology to integrate advanced analytics into business processes, such resources are indispensable. Lacking that skill, the organization may lose confidence in the ability of the program to perform as intended and the commitment to the program could wane.

For an analytics program to be effective, it is not sufficient merely to design an algorithm and then leave it untouched to operate indefinitely. Rather, it has to be updated regularly as circumstances change. Programs must be alert for routines that are generating large populations of false positives, which require time and resources to examine. The use of cognitive, machine-learning systems will provide companies with the means to continuously improve their analytics and make them more efficient for the purpose. These techniques require considerable time and effort by the company.

## Anti-fraud analytics must be ethical

The fourth trust anchor of trusted anti-fraud analytics concerns the **ethical integrity** of the process. Is its use considered acceptable by such stakeholders as employees, suppliers, customers, business partners and regulators? This, we believe, is the most important of the four anchors because it addresses some of the most sensitive areas of the relationship between the company and its stakeholders, in which trust plays a vital role. This is not simply a legal matter. A company could be fully compliant with the law and yet, if it were to adopt a heavy-handed approach to fraud detection, it may undermine the trust of its employees in the organization and other parties that are included in the detection scope.

These issues are particularly relevant in the emerging field of behavioral analytics. Until recently, the use of analytics to detect fraud focused on transactions. In the future, however, a growing emphasis is likely to be placed on analyzing the behavior of employees. This adds an additional layer of anti-fraud detection to the analysis of transactions by monitoring employees for possible behavioral anomalies that might lead to the perpetration of fraud.

One example of this is in the field of threat analysis. In the US, certain federal agencies and contractors are setting up programs to manage insider threats by monitoring employees' use of computers.

While this is an example of corporate surveillance at one end of the spectrum, the fact is that any anti-fraud program will be more effective if it operates with the consent and the trust of the company's stakeholders, most notably its employees, as well as third parties that do business with it.

This issue has to be handled carefully, depending on the culture in which the company is operating. In our report, *Global profiles of the fraudster*, many of KPMG's forensics experts around the world pointed out a prevalent culture among companies to trust their employees to do the right thing. There is a prevailing mentality that executives and most employees should be given the benefit of the doubt. According to the forensics experts, corporate leaders fear that if employees perceive that the company is using analytics to 'snoop' on them, this may undermine the trust between the company and its employees. This may make the management reluctant to deploy a behavioral analytics program.

How can this problem be surmounted? Successful implementation of such a program starts with the leadership clearly explaining the purpose of the anti-fraud analytics program and its intention to protect the reputation of the company as a whole, not to victimize (or benefit) individuals or particular groups. It is often easier to explain this to employees after a significant case of fraud has been uncovered, when people are more open to the idea of preventing a recurrence.

Companies may also decide that portions of the data under analysis could be anonymized, and only if a pattern of business behavior raises a red flag would the information about the individual responsible for the pattern of behavior be disclosed to investigators. If the information gathered in this way is used for a purpose other than combatting fraud and word leaks out, trust in the program will evaporate quickly. The key element here is transparency: if corporate leaders explain its purpose clearly and operate it strictly in conformity with the stated intent, the program will enjoy the trust of all stakeholders.

# Building a better culture

In this context, it is important to balance surveillance and transparency. An organization might conduct a strong surveillance program and a low level of transparency or any possible combination of the two, depending on the nature of the relationship between the company and its employees and other stakeholders. An organization that handles a lot of sensitive information or in which individuals handle large amounts of money is likely to have a stronger surveillance program than one that does not. If an organization is transparent about the nature of the analytics program it uses to monitor its operations and processes and adheres strictly to the ethical management of its analytic processes, it is likely to be trusted in how it conducts its anti-fraud measures.

Societies and the companies within them are experiencing a trend toward greater transparency. Stakeholders are demanding more openness from companies and other institutions. Social media is providing channels for publicizing more private information about individuals and organizations than ever before. However, greater transparency has two different facets in the context of this article. If companies are open with their stakeholders about their anti-fraud programs and adhere closely to the stated purpose, then trust will strengthen. But if the program veers off course and it becomes known that information collected is used for a different purpose, then the trust will be lost very quickly. Ensuring enough transparency to protect and maintain trust while guarding against sharing too much information, so as to aid a fraudster in avoiding detection, is a very difficult balancing act.

People must be confident that the analytics algorithms work as intended and must trust each other to use them properly. It's a weighty task but, if successful, we believe it will build a stronger, more compliant culture in the organization.

Join us in the discussion on LinkedIn or Twitter @KPMG.

## Where KPMG has helped:

### Deep pattern analysis algorithms for security anomaly detection

**Client challenge**

A global retailer's database systems were compromised by a cyber-attack that exposed sensitive non-financial data of a segment of its marketplace users. Hackers gained unauthorized access to marketplace user data by using employee credentials.

**KPMG response**

Following incident discovery and remediation, the client engaged KPMG in the US to assist with enhancing their Security Command Center (SCC) monitoring capabilities.

**Benefits to client**

The client is better able to detect network abnormalities in real time and has greater understanding of network activity. The client is better able to recognize anomalous network activity, inappropriate applications or applications using unusual ports by tracking network traffic in real time.

# About Global Data & Analytics at KPMG

In a global environment defined by constant disruption, business leaders need data and analytics they can trust to inform their most important decisions. KPMG's Data & Analytics (D&A) team has earned that trust with an evidence-based, business-first approach that's at our core. For more than 100 years, we have worked across industries to help member firms' clients address their long-term, strategic objectives. And as an internationally regulated accounting and professional services network, our member firms have an unwavering commitment to precision and quality in everything we do.

# Contacts

**Fernando Cuñado**
Head of KPMG Forensic
E: fcunadokpmg.es

**Juan Arenas**
Director
KPMG Forensic
E: jarenas@kpmg.es
T: +34 91 451 30 42

**Juan Mazarredo**
Director
KPMG Forensic
E: jmazarredo@kpmg.es
T: +34 91 451 30 33

**Marisa Yepes**
Director
KPMG Forensic
E: myepes@kpmg.es
T: +34 91 456 80 63

**María Barcenilla**
Manager
KPMG Forensic
E: mbarcenilla@kpmg.es
T: +34 91 456 60 33

**Carlos Ferrer**
Manager
KPMG Forensic
E: carlosferrer@kpmg.es
T: +34 91 456 82 61

**kpmg.com/data**

**kpmg.com/socialmedia**

**kpmg.com/app**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Publication name: Using analytics successfully to detect fraud
Publication number: 133602-G
Publication date: August 2016