Shifting into high gear: mitigating risks and demonstrating returns

Global Forensic Data Analytics Survey 2016

EY
Building a better working world

Contents

Foreword	3
Executive summary	4
01 Demand growing across the board	6
02 A maturing FDA landscape	12
03 FDA deployment: what are the key hurdles?	21
04 What does good look like?	24
05 Embracing the FDA revolution: going the distance	32
Survey approach	34
Contact information	35

Foreword

Forensic data analytics (FDA) has evolved considerably over the past two years. In our 2014 survey, we found that, although companies were deploying some forms of FDA, many were missing opportunities to leverage emerging advanced tools that would enable them to greatly strengthen and improve their risk management and investigative response programs.

In today's digital world, there are rapidly expanding opportunities for innovation and growth. Unfortunately, these new opportunities have also brought new fraud risks in the forms of cyber breaches and internal threat.

The mission-critical nature of information and the ease of digital access make organizations particularly vulnerable to cyber criminals and malicious insiders. Increasing regulatory pressure further compounds the need to address these risks with rigor.

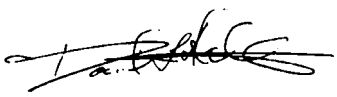
On the upside, advanced data analytics tools are becoming mainstream. New technologies and surveillance monitoring techniques are being developed to help companies manage current and emerging fraud risks, and there is growing awareness of FDA's benefits at the executive and board levels.

As a result of these push and pull factors, the demand for FDA investment has never been higher, and FDA deployments are maturing. Organizations recognize the value of FDA, and many are realizing positive results by deploying advanced technologies against meaningful volumes and varieties of data.

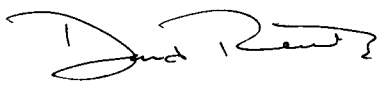
But companies need to recognize the full spectrum of value that FDA can bring — far beyond fraud detection — and be more aggressive in its implementation. Although senior management has gained much appreciation for the value of FDA, they need to adopt it beyond the scope of traditional fraud risk management, take action, and invest in the right skills and technologies to realize its potential.

This report is based on interviews with 665 executives between June and September 2015, augmented by the insights of our global Fraud Investigation & Dispute Services (FIDS) practice. We hope it helps businesses understand and articulate the compelling business case for FDA and harness FDA's full potential in managing risk.

We would like to thank all of the respondents and business leaders for taking the time to participate in this survey and for their valuable contributions, observations and insights.



David Stulb
Global Leader
Fraud Investigation & Dispute Services



David Remnitz
Global Leader, Forensic Technology & Discovery Services
Fraud Investigation & Dispute Services

Executive summary

01 Demand growing across the board

Organizations are looking to use FDA due to concerns over growing current and emerging threats, as well as the increasingly complex regulatory environment. Across all industries, the fastest-growing threats in the fraud risk universe are from cyber breaches and insider threats – and respondents recognize the importance of harnessing FDA to respond to these new threats.

Executive corporate management is listed as the top beneficiary of FDA as indicated by 73% of the respondents, followed by Internal Audit and the Board at 69% and 68%, respectively. Perhaps not surprisingly, C-suite respondents also indicate a greater sense of urgency around FDA adoption with 74% agreeing they need to do more to improve their current anti-fraud procedures, including the use of FDA tools, as compared to 69% for non-C-suite respondents.

02 A maturing FDA landscape

Focus on major FDA deployments is growing compared to our 2014 survey results, with higher levels of spending on advanced tools and proactive surveillance monitoring of larger volumes of data from a wider variety of sources. To get the most out of these sophisticated tools, organizations are increasing their in-house capabilities as indicated by a 22% increase in the number of in-house deployments as compared to the 2014 survey. In response to this trend, we also see leading technology companies introducing anti-fraud, surveillance monitoring and insider threat product offerings designed to address wide varieties of fraud and litigation risks across the enterprise.

Despite improving maturity overall, many organizations lack an understanding of the wide spectrum of value that FDA can deliver – and few are fully realizing the potential of their FDA deployments, particularly around the cost savings and efficiencies gained from the use of FDA. When asked about the main benefits of using FDA, 79% indicate the ability to detect fraud that they couldn't detect before, and 78% indicate earlier fraud detection; however, only 42% indicate reduced costs of their anti-fraud programs.

03 FDA deployment: what are the key hurdles?

Senior management can see the need for FDA to address key business risks but are proving reluctant to fund it. Two years ago, 64% of our respondents felt that their investment in FDA was sufficient; this year, only 55% are confident they are spending enough. This discrepancy between perception and practice is partly because decision-makers aren't aware of the broad range of business value that FDA can deliver.

FDA success can be improved by:

- **Articulating the business case for FDA to management** – When articulating the return on investment, companies need to focus on the full spectrum of value that FDA can deliver, including cost reduction and improved risk management.
- **Building teams with the right skills** – Successful deployments require technical skills, domain knowledge and data analytics expertise, yet few organizations have all of these skills in place.
- **Deploying the right technology** – While we have seen an increased level of adoption of advanced FDA technologies, there is still a substantial number of companies that are not using them. Many of those tools are vital for analyzing large quantities of multi-format data.

04 What does good look like?

Our survey found those organizations receiving positive results from FDA have a number of elements in common. They are more likely to:

- **Use advanced technology**

  In almost every circumstance, those companies using more sophisticated analytics, beyond basic spreadsheet-type, rules-driven tests, report better fraud detection in less time. These successful FDA deployments are harnessing sophisticated analytics tools, including social media and web monitoring, voice searching and analysis, and visualization and reporting tools.

- **Analyze more data**

  We have observed a positive correlation between the use of large data volumes (over 10 million records) and achieving positive results of FDA implementation. The same is relevant to data variety, with those reporting positive results also applying a much broader array of both structured and unstructured data sources.

- **Invest more of their total compliance and anti-fraud spend in FDA**

  Our survey found those reporting positive results invest one-third of their total anti-fraud program budget on FDA.

Around the world, many leading organizations are harnessing the full benefits of FDA, but others are struggling to do so. Boards and senior-level management who see FDA's potential, but have yet to come to terms with the investment required, need to understand the broad range of value that sophisticated analytics can deliver. Once this is appreciated, the business case for FDA becomes clear.

What do we mean by forensic data analytics?

In this document, FDA refers to the ability to collect and use data, both structured (e.g., general ledger or transaction data) and unstructured (e.g., email, voice or free-text fields in a database), to prevent, detect, monitor or investigate potentially improper transactions, events or patterns of behavior related to misconduct, fraud and noncompliance issues.

What is cybercrime?

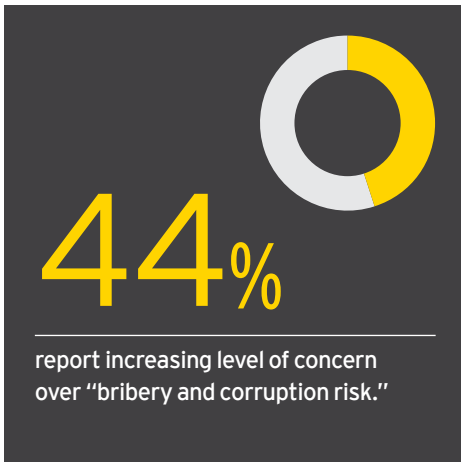
In the context of this survey, cybercrime is the use of a computer and its network to commit fraud such as illicit transferring of funds, disrupting critical business operations, or stealing intellectual property (IP), confidential personal data and other critical digital assets.

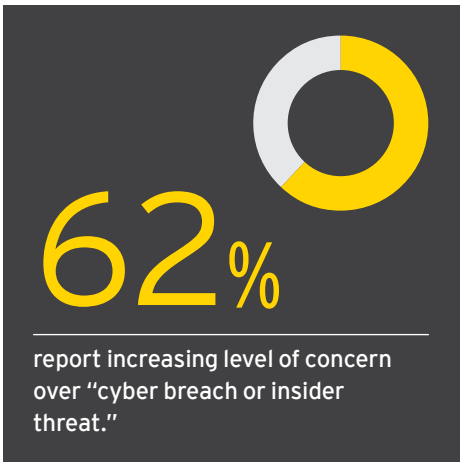
What is an insider threat?

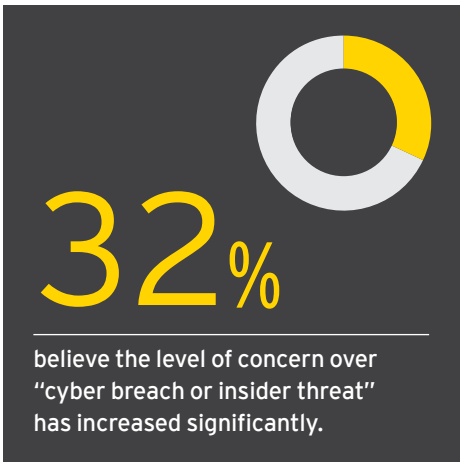
A current or former employee, contractor or business partner with authorized access to an organization's network system or data who intentionally uses this access to compromise the confidentiality, integrity or availability of the organization's data or information systems. Insider threats can include fraud, IP theft, unauthorized trading, espionage or information technology (IT) sabotage – where a malicious insider disrupts information systems, breaches confidentiality or destroys or corrupts data.

Demand growing across the board

Current and emerging risks are converging to create greater urgency for organizations to use FDA. Cybercrime, insider threats and aggressive regulatory pressure make FDA a growing priority for boards and senior management.



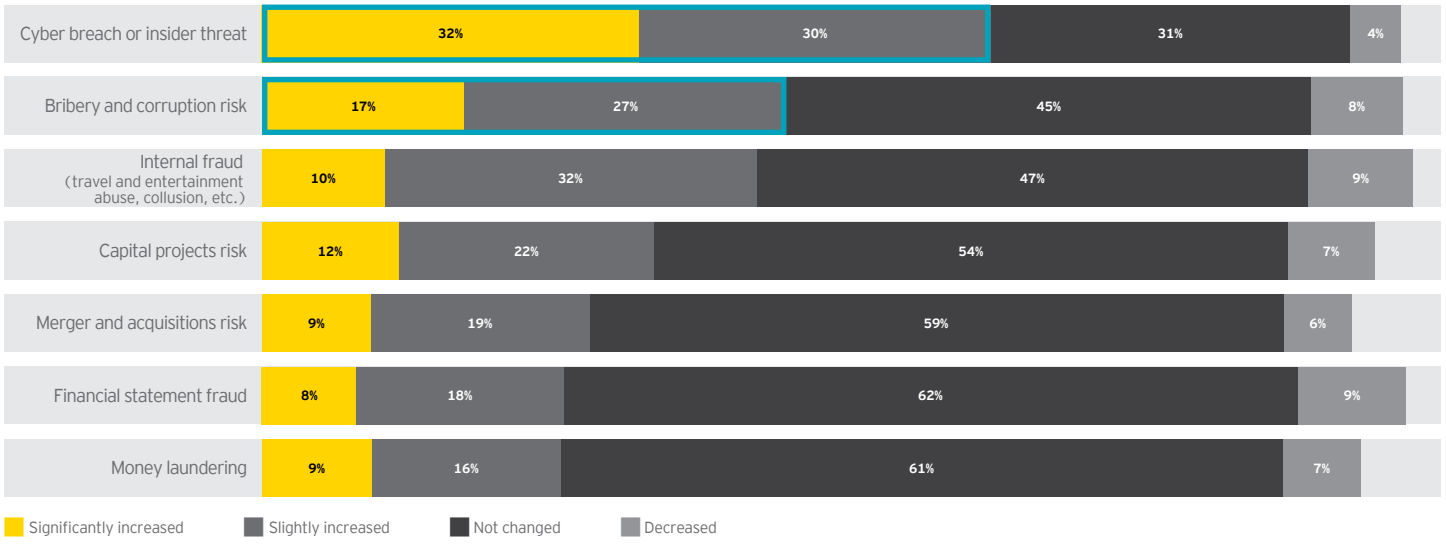




Current and emerging risks driving demand

This year's survey revealed the fastest-growing threats in the fraud and investigative risk universe are from cyber breaches and insider threats, which include malicious insiders stealing, manipulating or destroying data. Historically, responsibility for managing cyber and insider threat risks falls to an organization's IT and security departments – not those represented in our survey, who are responsible for the anti-fraud and compliance programs. Yet 62% of our respondents report increasing level of concern regarding this area, while 32% believe it has increased significantly.

Figure 1: Cyber breach or insider threat is clearly top of mind



Q. Over the past two years, how has the level of concern about each risk area changed in your organization?
Base: All respondents (665)

The "Don't know" percentages have been omitted to allow better comparison among the responses given.

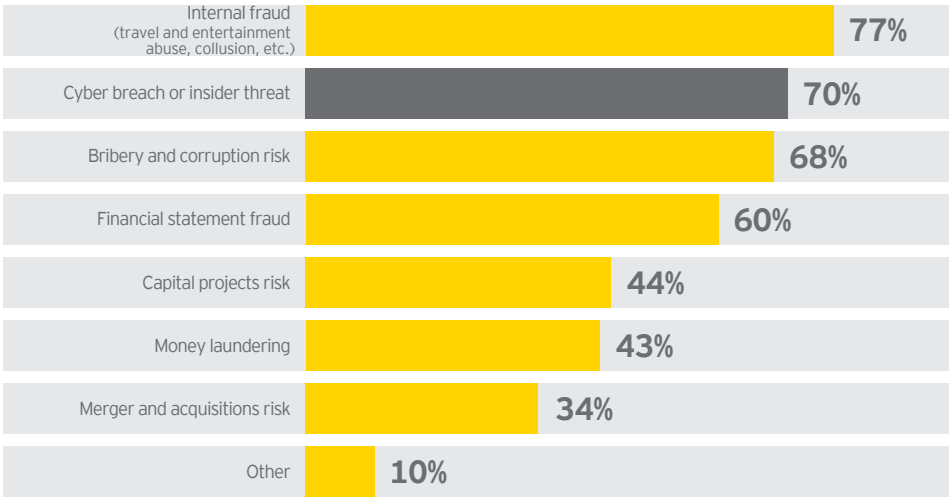
Concerns about cyber and insider threat extend across industries. Nine out of nine industries rate the threat of external and internal cyber breaches as their top risk.

This strong consistency in the perception of cyber threat is not surprising now that cyber attacks (both internal and external) are a fact of life for business, posing a dynamic, relentless challenge for leading companies. With a growing imperative to protect digital assets — not just physical ones — our respondents see FDA as playing a critical role in managing a broader spectrum of risks. Interestingly, "cyber breach or insider threat" is the second-highest risk area where 70% of respondents are using FDA. "Internal fraud" risk, an area that has long been managed using FDA, was ranked as the top use case at 77%.

Figure 2. Perceived risks by industry — the percentage of respondents who have seen the increased level of risks

	Cyber breach or insider threat	Bribery and corruption risk	Internal fraud (travel and entertainment abuse, collusion, etc.)	Capital projects risk	Merger and acquisition risk	Money laundering
Financial services	74%	50%	47%	24%	25%	46%
Life sciences	63%	49%	49%	42%	29%	19%
Transportation	46%	46%	38%	38%	33%	29%
Manufacturing	48%	35%	32%	32%	24%	18%
Consumer products, retail and wholesale	64%	38%	42%	35%	21%	23%
Technology, communications and entertainment	55%	48%	49%	34%	29%	17%
Oil and gas	61%	52%	35%	35%	37%	19%
Mining	52%	37%	30%	30%	33%	11%
Power and utilities	56%	41%	34%	46%	44%	10%

Figure 3. Top fraud risks using FDA



Q. **In which of these risk areas or types of fraud does your company use FDA when investigating incidents and/or monitoring risks?**
Base: All respondents (665)

Multiple answers allowed, may exceed 100%.

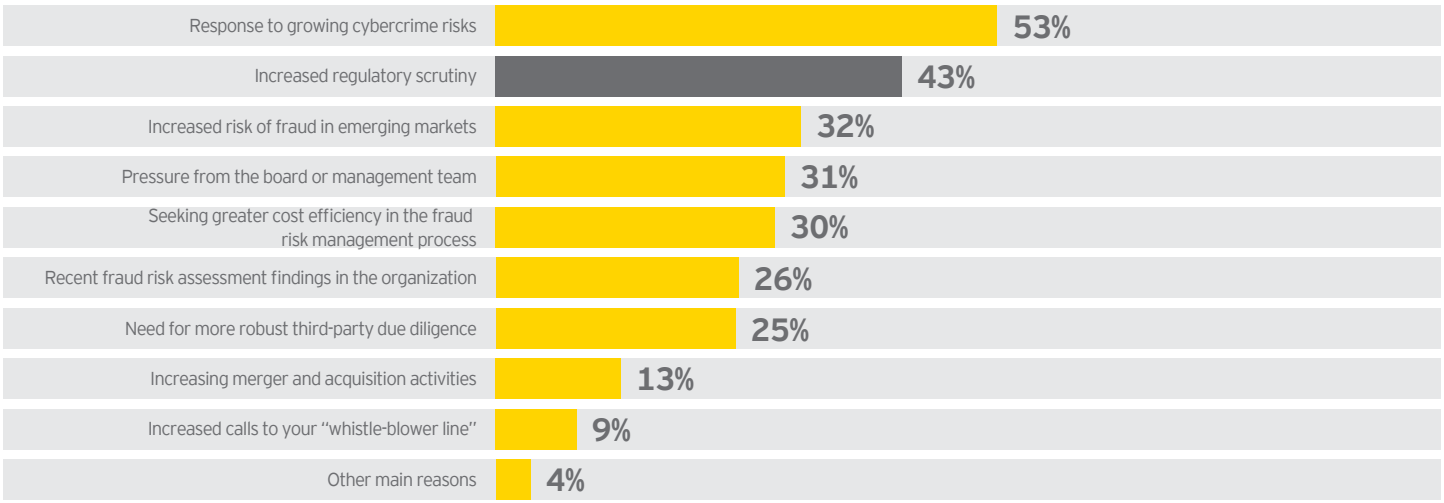
Regulatory enforcement becoming more rigorous and widespread

FDA demand is also being driven by increasing government and public scrutiny of fraud risk, with 43% of respondents citing regulatory pressure as one of the main reasons behind their investment in FDA, second only to responses to growing cybercrime risks. C-suite respondents are more likely to be concerned about regulatory pressure. This is not surprising considering that high-profile regulatory enforcement actions have been dominating the headlines, leading to billions of dollars in fines and the prosecution of individual executives.

43%

of respondents cite regulatory pressure as one of the main reasons driving their investment in FDA.

Figure 4. Top drivers of FDA investment



Q. **What are the main reasons that you are planning to increase your investment in FDA capabilities?**
Base: Respondents who plan to increase investment in FDA (405)

Multiple answers allowed, may exceed 100%.

The United States Securities and Exchange Commission (SEC) and Department of Justice continue to lead the way in robust domestic and extraterritorial enforcement actions. The SEC's Financial Reporting and Audit Task Force is now deploying cutting-edge FDA tools to mine data for fraud and is engaging whistle-blowers in unprecedented numbers to uncover financial reporting and disclosure problems.

> "At the SEC, we have made great strides in leveraging data and technology to detect and pursue misconduct. In the enforcement arena, the Commission is using data analytics to help identify wrongdoers and conduct streamlined investigations to optimize our resources."
>
> **SEC Chair Mary Jo White, opening remarks at the 21st Annual International Institute for Securities Enforcement and Market Oversight, 2 November 2015**

monetary remedies in this past fiscal year

Outside the United States, regulators in the United Kingdom, Germany, Italy and France, among others, have been involved in major enforcement actions. In Asia, prosecutions for corruption are increasingly frequent, with China leading the way.

Parallel investigations are also becoming more common, with the European Commission and Japanese regulators teaming with their US counterparts on cartel investigations. Cross-border cooperation among prosecutors is strong and will only strengthen as emerging markets, including India, Brazil and many Asian countries, pass anti-bribery/anti-corruption legislation or take steps to bolster their enforcement efforts.

Increased urgency by C-suites to adopt FDA

The cost of getting it wrong is becoming too grave to ignore. Facing the severity of fraud risks and the threat of regulatory enforcement, C-suite respondents have a stronger sense of urgency around FDA adoption than other executives. Overall, 69% of respondents agree with the statement: "We need to do more to improve our current anti-fraud procedures, including the use of FDA tools." But this percentage jumped to 74% for the C-suite cohort.

In addition, 31% of respondents say one of the main reasons to increase FDA investment is pressure from the board or management team. They also cite corporate executive management and the board as the first- and third-highest beneficiaries of FDA activities, moving up from second and fifth, respectively, two years ago.

74%

of C-suite respondents

"We need to do more to improve our current anti-fraud procedures, including the use of FDA tools."

"As we look toward COSO guidance around conducting fraud risk assessments as part of an effective internal controls framework, we will see a strong emphasis on the use of forensic data analytics."

Vincent Walden, Partner, Forensic Technology & Discovery Services, FIDS US, EY

Case studies

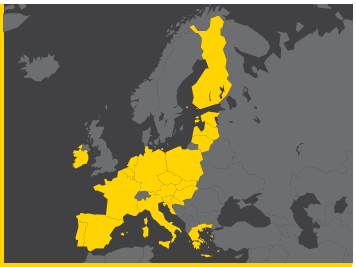
Data-driven financial reconstruction in a regulatory investigation

Industry: **Manufacturing**
Country: **United States**

The situation:
A publicly traded technology manufacturer received a subpoena from a regulatory authority alleging improprieties around revenue recognition.

How FDA helped:
The use of FDA helped the investigation team model the order-to-cash process, including sales orders, invoices, receipts, shipping, discounts and rebates. The team then executed tests to isolate the timing of certain transactions and identify high-risk customers for further inquiry. Advanced FDA techniques included using text analytics to analyze the free-text notes column in the order entry system to understand the nature of payments and identify suspicious language or corrupt intent. As a result, the company was able to analyze 100% of the sales data within the time period for which they were required to respond to the subpoena and run targeted tests to evaluate the sufficiency of the regulator's claims on an expedited basis.

Fraud investigation– financial loss assessment



Industry: **Power and utilities**
Country: **Eurozone**

The situation:
A multinational utilities company faced major financial loss for fraudulent credit notes and the manipulation of billing data.

How FDA helped:
The project team collected and analyzed nearly 1 TB of data from SAP IS-U (SAP Module for Utilities) to assess the losses and potential impact on the organization and to identify control weaknesses for immediate remediation. They first conducted a data mining and clustering procedure to understand the variety of billing and credit entry processes. The analyses were then used to identify potential fraud patterns by applying statistical methods and customized data analytics. The results revealed more fraud patterns and the fact that outside collaborators were involved. The outcome helped the company assess the damage for insurance claim purposes and take immediate actions to implement remediation procedures within its control environment. The company now plans to implement a monitoring program leveraging the FDA tools developed during the investigation.

2

A maturing FDA landscape

Many organizations are increasing their focus on FDA deployment, with increased spending on advanced tools and proactive monitoring of larger volumes of data. However, some are failing to recognize that the value FDA can bring to anti-fraud programs goes beyond just detection and investigation.

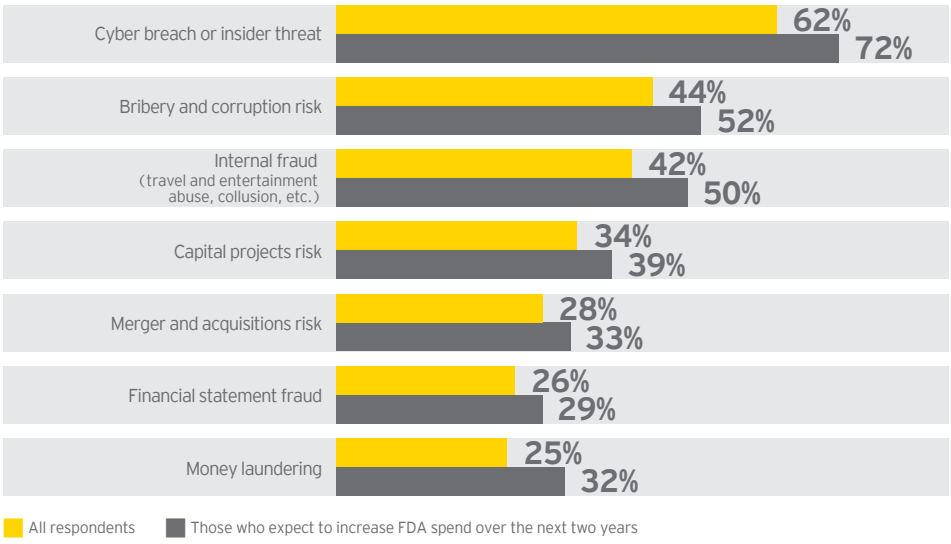
Companies want to spend more on FDA to manage today's risk

Growing organizational demand for greater FDA investment is being driven by awareness of the value it can deliver and emerging risks. We expect this trend to continue into the future as data volumes and varieties continue to expand, more technologies become available and regulatory scrutiny increases. Two years ago, 64% of our respondents felt their investment in FDA was sufficient; this year, only 55% are confident they are spending enough.

Three out of five respondents plan to increase their spend on FDA over the next two years. We see a clear correlation between the respondents' FDA spend and their perceptions of risk in the chart below.

of respondents think their FDA spend is sufficient.

Figure 5: Risk driving spend: correlation between the FDA spend and perceptions of increased level of risk



Q. **Over the past two years, how has the level of concern about each risk area changed in your organization?**
Base: All respondents (665); those who expect to increase FDA spend over the next two years (406)

Multiple answers allowed, may exceed 100%.

of respondents plan to spend more on FDA.

Companies working with data sets that push the limit of traditional spreadsheet tools (i.e., more than 10 million records) are also more likely to be planning significant increases in their FDA spend. In contrast, only 13% of those analyzing fewer than 1 million data records are planning to significantly increase investment in FDA.

> "In my opinion, we need to invest more money to get the best forensic data analysis tools that are available in the market."
>
> **Head of Internal Audit, Capital Markets, France**

63%

of respondents

spend at least half of their FDA investment on proactive initiatives

Companies are investing more of their FDA spend on proactive initiatives

Given so much management focus on fraud prevention, this year's survey included a new question to gauge how much of a company's FDA activities are proactive — as opposed to merely reacting to an investigation or adverse event. The results are striking. Sixty-three percent of the respondents are investing at least half of their FDA spend on proactive monitoring initiatives.

We believe this strong proactive stance is in response to regulatory enforcement concerns, as well as improved surveillance analytics and compliance monitoring offerings in the market. With governments imposing substantial monetary penalties — sometimes accompanied by prison sentences for executives — organizations have every incentive to improve their FDA programs to better prevent and detect fraud.

Companies investing in proactive activities also understand the value of FDA in reducing the costs of anti-fraud programs. According to the Association of Certified Fraud Examiners' most current *Report to the Nations on Occupational Fraud and Abuse*, those companies with proactive data analytics in place saw a cost per fraud incident that was 59.7% lower (roughly US$100,000 lower per incident) than those companies not using proactive data analytics — more than any other control listed in the survey. Further, the median duration of a fraud incident with respect to the presence of proactive data analytics was half the time — 12 months versus 24 months.

Growing sophistication in technology and the use of data

Technology maturity is also growing. The use of visualization tools has doubled since our 2014 survey. Respondents also report the increasing use of social and web monitoring tools and statistical analysis and data mining packages.

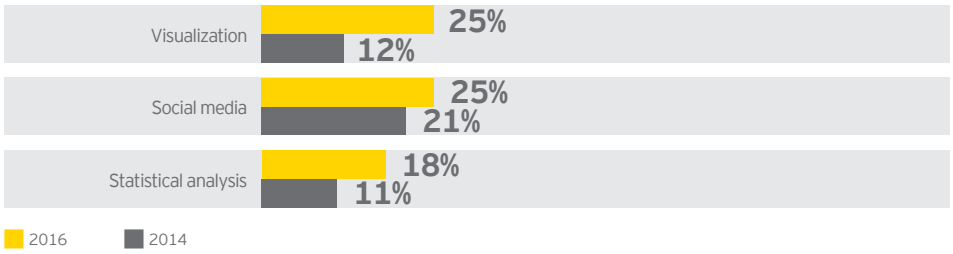
Half of the respondents, however, report that their adoption of advanced analytics technologies remains immature. For example, spreadsheets are still the most common tool used to manage fraud risk, with more than three-quarters of respondents indicating their use. Clearly, there is still more work to be done.

The nature, variety and complexity of structured and unstructured data is changing at an exponential rate — causing companies to rethink how they monitor rogue or noncompliant activities. The Internet of Things has added another dimension to the data. In many organizations, machines are communicating with other machines without human involvement. Employees are often communicating outside corporate networks using social media, mobile phones or web logs. All of these scenarios exemplify how traditional monitoring or investigative analytics techniques deployed a decade ago may no longer be as effective given the nature, variety and complexity of data in today's organizations.

Given that unstructured content accounts for around 90% of an organization's digital information,[1] it's encouraging to see that 75% of respondents routinely analyze a wide range of structured and unstructured data. Businesses can yield great benefits by combining structured and unstructured data (emails, file metadata, audio and video files, etc.) in their analysis to gain a comprehensive view of their risk environment. For example, comments from sales logs can show an individual's intent to commit a fraud, while a financial transaction can provide the evidence.

[1] *Unlocking the Hidden Value of Information,* IDC website, www.idc.com/getdoc.jsp?containerId=prUS24993814, accessed 23 November 2015.

Figure 6: The increasing adoption of advanced FDA technologies



Q. **Which FDA tools do you utilize in managing fraud risk?**
Base: 2016 all respondents (665); 2014 all respondents (466)

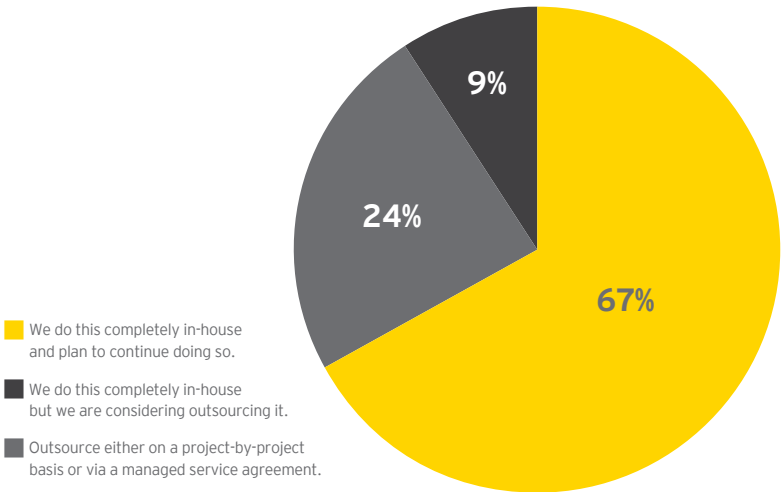
Multiple answers allowed, may exceed 100%.

Multiple deployment options

Increasing numbers of organizations are bringing FDA deployment in-house. Respondents conducting FDA completely in-house increased from 45% two years ago to 67%. In the last two years, leading technology companies have also responded to this growing in-house FDA trend by introducing enterprise-class surveillance and insider threat capabilities to help companies better prevent, detect, monitor or investigate potentially improper transactions, events or patterns of behavior related to misconduct, fraud and noncompliance issues.

For example, IBM has introduced IBM Counter Fraud, and SAP has introduced SAP Fraud Management. SAS has also strengthened its offering around its Fraud & Security Intelligence solution. However, deploying these new software capabilities, whether in-house, via the cloud or through a managed service model, requires a multidisciplinary group of professionals who have domain and subject matter knowledge (to ask the right business questions), data science and data management expertise (to translate business questions into meaningful analytics), as well as systems and IT infrastructure expertise (to maintain and secure the platform for use).

Figure 7: Multiple deployment options



Q. **Which deployment model best describes how you conduct FDA as part of the company's anti-fraud program?**
Base: All respondents (665)

Top challenges faced by those currently considering outsourcing:

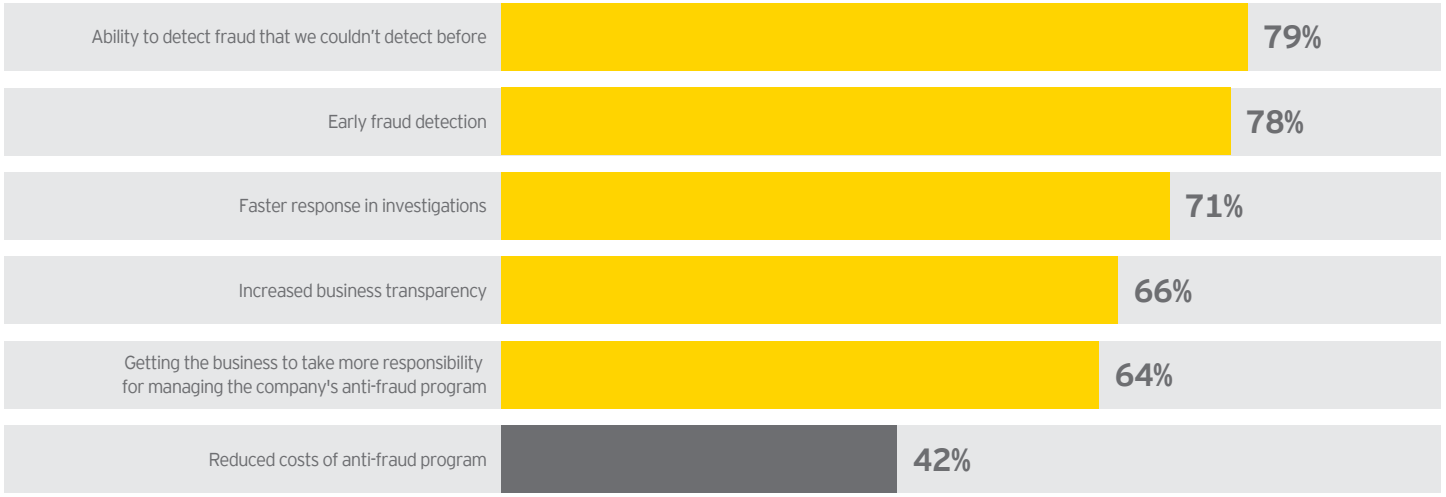
- Challenges in combining data sources
- Lack of budget and resources
- Lack of expertise
- Inadequate technologies currently in place

Notably, a large percentage of companies are also seeking outside help for FDA, either on a project-by-project basis or through managed service arrangements. Twenty-four percent of respondents are already outsourcing either as projects or as a managed service; another 9% are considering it. In these circumstances, the benefits of outsourcing outweigh the large capital investment required to build in-house FDA technologies and skill sets. Outsourcing enables the companies to quickly ramp up their FDA capabilities and focus on the analytics consumption and interpretation. The finding is consistent with IDC's market forecast for business analytics process outsourcing services, which estimates a 14.2% compound annual growth rate through 2019.[2]

Organizations are not recognizing the full spectrum of value FDA can deliver

Despite the risk universe evolving, the main perceived benefits of FDA have not changed to keep pace. In line with our survey's findings two years ago, respondents continue to identify the top three perceived benefits of using FDA in their anti-fraud programs as "ability to detect fraud that we couldn't detect before," "early fraud detection" and "faster response in investigations."

Figure 8: Main benefits of FDA — not fully realized



Q. **What do you think are the main benefits of using FDA in your anti-fraud program?**
Base: All respondents (665)

The "Other" percentages have been omitted to allow better comparison among the responses given. Multiple answers allowed, may exceed 100%.

As indicated in Figure 8, although the top three selected benefits of using FDA are clearly important, both from risk mitigation and cost avoidance perspectives, it is surprising to see how few respondents selected "reduced costs of anti-fraud program." Only two in five see the potential for FDA to reduce the costs of their anti-fraud programs as a main benefit. By using current technology capabilities and leading analytics to help focus investigative and compliance monitoring efforts, FDA can be an important enabler of cost reduction.

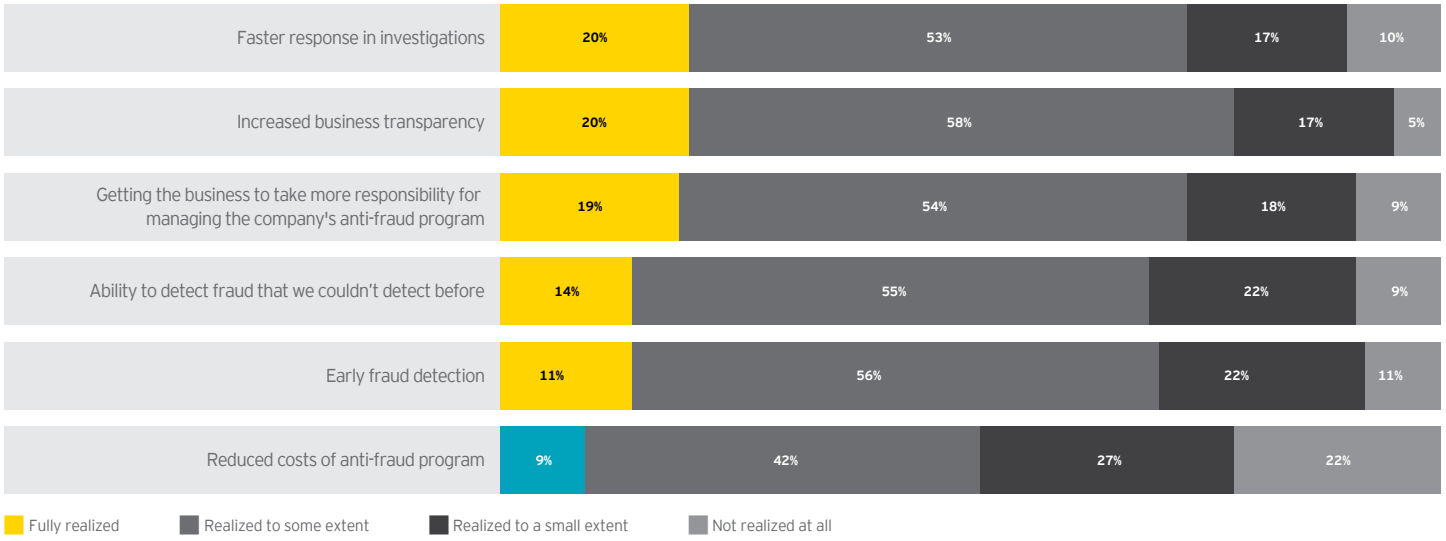
[2] *IDC Worldwide Business Analytics Services Forecast, 2015–2019, November 2015.*

"[We need to] ... promote a culture of risk management and use of analysis in the areas of anti-fraud across all divisions in the company, not just at the central management level."

Internal Audit Executive, Retail and Wholesale, Italy

Across the board, the majority of respondents believe they have a long way to go to reap the full value of FDA in reducing program costs, with only 9% confident that they are fully realizing the benefit.

Figure 9: Realizing the full benefits of FDA



Q. **To what extent have you realized the benefits of FDA over the past two years?**
Base: All respondents (665)

"We continue to see the global impact of cyber breach both from internal and external threats. The monitoring and analysis of an organization's structured and unstructured data assets will be fundamental to the early detection and investigation exercise."

Paul Walker, Partner, Forensic Technology & Discovery Services, FIDS UK, EY

Case studies

Proactive fraud risk assessment and testing

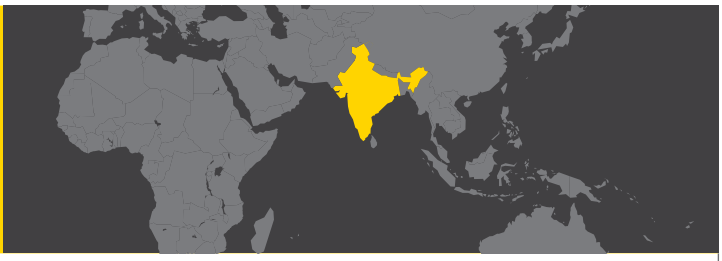
Industry: **Life sciences**
Country: **European company with operations in Asia-Pacific, Eastern Europe, Middle East, Africa and Latin America**

The situation:
A multinational life sciences company sought a global compliance and anti-bribery/anti-corruption monitoring program and wanted to leverage the data from its highest-risk markets to proactively identify risks and improve its audit sampling.

How FDA helped:
The project team collected and analyzed data from various systems of multiple business units in more than 10 countries across the globe. They built tailored dashboards for each market, including transaction and vendor risk scoring, comparative customer analysis and social network analytics, customized for local languages. The team also developed standardized data requests and extraction templates to facilitate future data analytics processes and compliance audits. The project enhanced the organization's global monitoring program by integrating multiple structured and unstructured data sources and designing tests that helped identify potentially improper payments to high-risk vendors, employees and distributors. Besides fraud detection and process improvements, the FDA efforts helped the audit and compliance team save time and money during fieldwork activities.

Risk review of distributor management system

Industry: **Consumer products**
Country: **India**



The situation:
A leading consumer products company based in India planned to perform a risk review of its distributor management system in order to identify vulnerabilities in its sales process and develop subsequent risk mitigation strategies.

How FDA helped:
The company, working with an outside professional services firm, developed fraud scenarios based on potential rogue transactions. The team analyzed sales transactions and other relevant data amounting to over 50 million records pertaining to the company's India distributors for a period of three years. Detailed risk analyses were carried out to identify high-risk distributors along with the associated financial implications for the company. Visualization dashboards were created to provide senior leadership with complete visibility across all of the distributors. Based on the outcome of the data analytics performed, the company is formulating a risk monitoring and control plan.

Financial statement audit

Industry: **Media and entertainment**
Country: **Australia**

The situation:
A media and entertainment company needed to better understand the risk of financial loss.

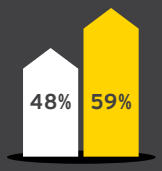
How FDA helped:
The company teamed with a professional services firm to develop a suite of analytics tests and data visualization dashboards across the accounts payable (AP) process, including employee-vendor relationships, duplicate payments, segregation of duties and delegation of authority. The dashboards gave the company great visibility over the internal controls and fraud risks by testing 100% of its AP transactions in a timely fashion. The company ultimately expanded the FDA deployment to include monitoring of additional processes and risk areas.

"We need to do more to improve our current anti-fraud procedures, including the use of FDA tools."

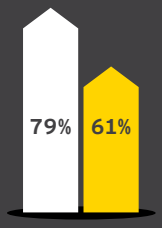
78% of respondents from emerging markets agree with the above statement, compared with 65% of organizations in developed markets.

Emerging markets versus developed markets

Respondents using FDA to actively address cyber breach or insider threat



Respondents saying their budget is "sufficient"



Respondents saying they need to improve management awareness of the benefits of FDA

79% of emerging markets respondents think that FDA could play a significant role in combating cyber and insider risks.

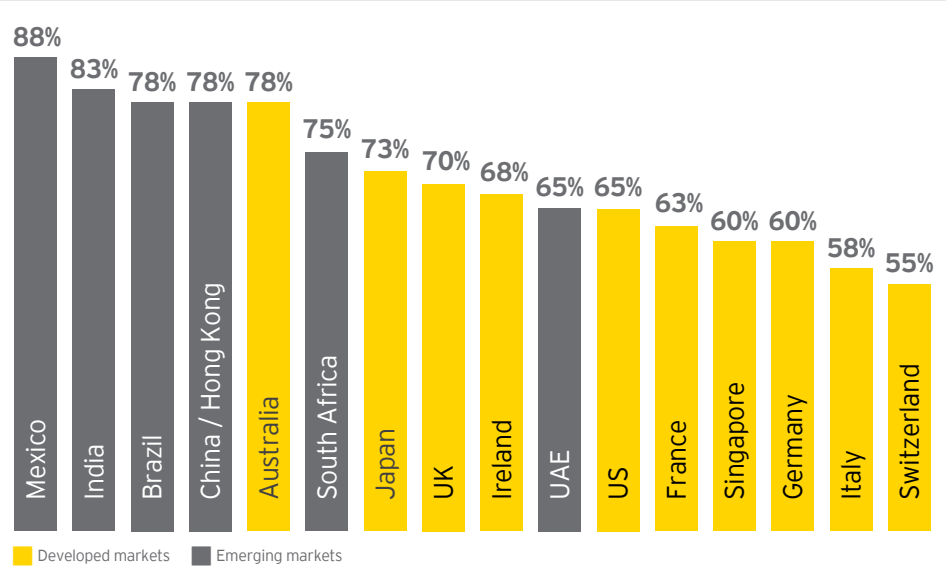
Emerging markets

Developed markets

Greater sense of urgency in emerging markets

Respondents in these markets have the greatest sense of urgency to adopt FDA. A much larger percentage (78%) of respondents from these markets agree with the statement: "We need to do more to improve our current anti-fraud procedures, including the use of FDA tools," compared with 65% of organizations in developed markets.

Figure 10: Perceived effectiveness by country



Q. To what extent do you agree that "We need to do more to improve our current anti-fraud procedures, including the use of FDA tools"?
Base: All respondents (665)

The sense of urgency, however, is focused more on using FDA to combat traditional fraud, such as bribery and corruption, than to address cybercrime or insider threat. Only 66% of respondents in emerging markets are using FDA to actively address cyber breaches or internal threats, compared with 72% in developed markets. This is not to suggest that organizations in emerging markets don't realize the potential for FDA to manage cyber and insider risks. On the contrary, 79% of emerging markets respondents think that FDA could play a significant role in combating cyber and insider risks. Focusing FDA investment on more traditional fraud risks is understandable given likely funding constraints and the underlying maturity of the local market.

Forty-eight percent of emerging markets respondents say their budget is "sufficient," compared with 59% of their peers in developed markets. The funding challenge is directly tied to management awareness. A significant 79% of emerging markets respondents say they need to improve management awareness of the benefits of FDA, compared with 61% in developed markets. The resulting focus of FDA investment on more traditional fraud risks rather than cybercrime or internal threats appears to be due to budgets and is clearly a gap to be bridged.

"In Asia-Pacific, we are seeing more and more companies investing in advanced forensic data analytics capabilities for effective compliance monitoring, as well as fraud prevention and detection."

Reuben Khoo, Principal, Forensic Technology & Discovery Services, FIDS Singapore, EY

3

FDA deployment: what are the key hurdles?

To realize FDA's full potential, organizations need to deploy the right technology and develop new skills. But to justify the investment required on both fronts, FDA proponents must be able to articulate a business case that demonstrates the full value chain of FDA.

Business context of FDA

When articulating the business value of FDA, the conversation needs to focus on the full spectrum of business value and stakeholder beneficiaries. Below are common use cases:

1. Regulatory and litigation response
2. Internal or cyber-breach investigations
3. Surveillance analytics
4. Internal and external audit support
5. Industry-specific fraud and compliance risk management

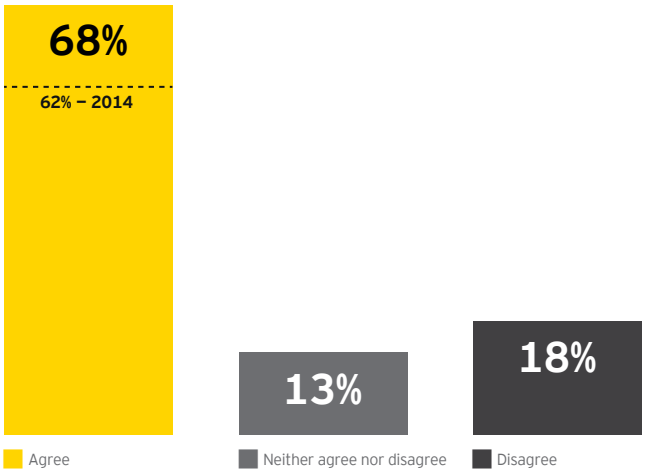
Making the business case for FDA to management

Our survey reveals that organizational reluctance to invest significantly in FDA is partly due to lack of management buy-in around its potential return on investment. Respondents believe they need to be better equipped to articulate the business case of FDA to management: 68% say they need to improve management's awareness of the benefits of FDA in their anti-fraud programs.

> "[We need to] ... educate management on what constitutes adequate funding. It's not just about support from management; they must recognize the need to invest in improving our fraud investigation capabilities."
>
> **Head of Compliance, Banking and Capital Markets, Singapore**

This finding highlights a discrepancy between perception and practice. In our survey, we found that senior management has an increased sense of urgency to adopt FDA, yet respondents also cite the need to educate this group on the need for sufficient investment. We believe the gap between perception (that management can see the need for FDA) and practice (their reluctance to fund it) can stem from the lack of awareness of the full spectrum of risk management benefits that FDA can deliver.

Figure 11: Growing need for management's awareness



Q. To what extent do you agree that "We need to improve management's awareness of the benefits of FDA in the company's anti-fraud program"?
All respondents (665)

The "Don't know" percentages have been omitted to allow better comparison among the responses given.

Building teams with the right skills

For successful deployment, the human element of FDA is an important consideration, requiring three distinct skill sets:

- **Technical skills** – to understand the organization's systems and advise on acquiring additional technology
- **Domain knowledge** – familiarity with the relevant risk areas in the business and the ability to interpret analytics results in the context of the organization
- **Data analytics (e.g., data science) expertise** – mathematical, computer science and business intelligence techniques, such as pattern recognition, statistical analysis, query design and data visualization

Yet few organizations have all of these skills in place, as evidenced by the emerging trend reported toward outsourcing. Although more than 80% of our respondents say their organizations have sufficient domain knowledge, about one-third lack data analytics expertise and nearly 40% lack technical skills. Clearly, one key enabler to realizing the full value of FDA is adequate training and expertise. To develop a comprehensive and effective FDA program, companies need to tie all three skill sets together – this typically involves teaming among compliance, legal, internal audit, the business and IT.

"We need a new IT team – analytics is a different area, and our operational staff are not analytics people. It is a different skill set."

CFO, Transportation, Singapore

Deploying the right technology

Respondents continue to rate "challenges in combining data sources" as the top issue to overcome in implementing FDA. This suggests that organizations need to think about their data holistically, deploy the right technology and promote the required skill sets. Building data sets that talk to one another is the first step to successful analytics.

Another sticking point for moving to more advanced tools appears to be budget, which our respondents rank as the second-largest FDA challenge – higher than in our previous survey. However, analytics technology has improved, making deployment and accessibility easier. For example, more "self-service" applications are available via the cloud that require less customization to implement. Further, significant improvements in computing power and scalability (i.e., Hadoop), combined with ever-decreasing storage costs, make the use of FDA more cost-effective. These developments help demonstrate the return on investment of FDA to senior management and should bolster the FDA business case.

According to Gartner, the need for data scientists is growing at about three times that for statisticians and business intelligence analysts, and there is an anticipated 100,000-plus-person analytic talent shortage through 2020.[3]

Don't forget the human element of your FDA program

"In 39% of leading analytics organizations – versus 12% of the rest – analytics skills are recognized, effective, efficient, monitored and clearly used to support decisions. More than one-third of the top 10% also have well-defined competencies for each role and level, along with robust training programs that address potential skills shortages."

EY and Forbes Insights, Data and Analytics Impact Index: don't forget the human element of analytics, 2015. http://www.forbes.com/forbesinsights/ey_data_analytics_2015/index.html

"The human element is perhaps the most important factor to achieving long-term success. To succeed, ask the right business questions that address key risks, and engage the stakeholders in the design. Only then should they map those questions to the right technology and data sources."

Chris Mazzei, Chief Analytics Officer, EY

[3] *Defining and Differentiating the Role of Data Scientist,* Doug Laney, Gartner 2012

What does good look like?

Not every organization is getting the full spectrum of value from FDA, but the ones that are have a number of elements in common. They are more likely to use advanced FDA tools that enable them to analyze larger volumes of data from a wide range of data sources, both structured and unstructured. They put a higher percentage of their total anti-fraud program spend into FDA, and they tend to focus on proactive activities, not just reactive ones.

Survey respondents who say they are currently getting positive results or recoveries from their FDA tools are more likely to:

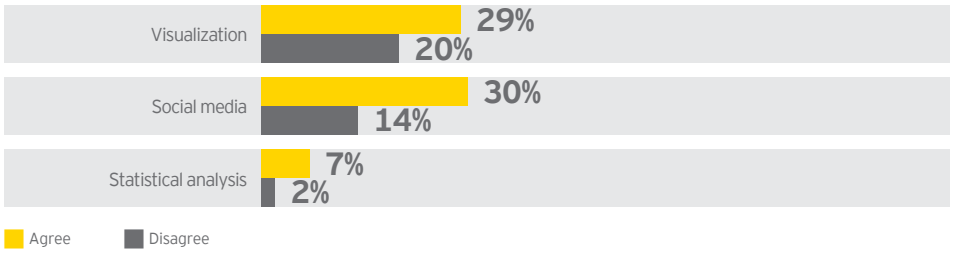
01 Use advanced technology

Companies that successfully deploy FDA harness sophisticated analytics tools. A much higher percentage of those who report positive results are using social media, web monitoring and visualization tools.

56% agree

"We currently get positive results or recoveries from the FDA tools that we use."

Figure 12: The use of advanced FDA technologies



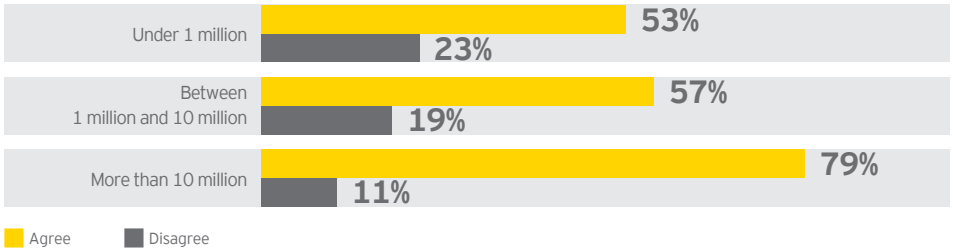
Q. What tools do you utilize in managing fraud risk?
Base: Among all respondents (665), 56% (370) agree and 21% (140) disagree that "We currently get positive results from the FDA tools that we use."

Multiple answers allowed, may exceed 100%.

02 Analyze large data volumes

More powerful analytics tools allow organizations to analyze more data, both in terms of volume and variety. Our survey shows a high correlation between reports of positive results and the use of large data volumes. Seventy-nine percent of those reporting positive results, versus 11% of those who don't, are using more than 10 million records, which are typically outside the domain of spreadsheets and thus require more sophisticated tools for analysis. Of those who are not seeing positive results with FDA, data volume analyzed is low, with only a small minority of respondents analyzing more than 1 million records. Companies are likely to see better results from their FDA tools when they start applying them to more of their data.

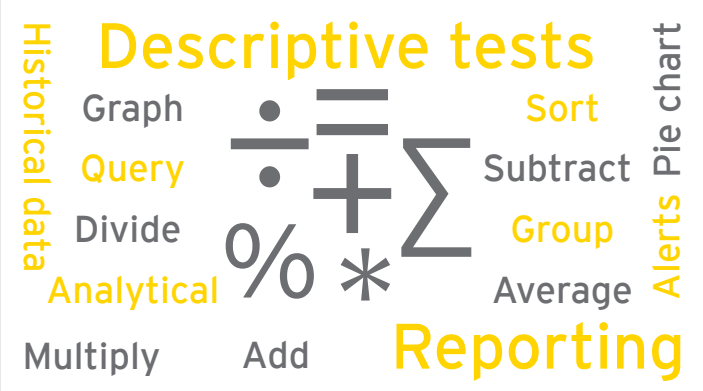
Figure 13: Data volume used in FDA



Q. What data volume (in records) do you typically work with in your FDA tasks?
Among all respondents (665), 56% (370) agree and 21% (140) disagree that "We currently get positive results from the FDA tools that we use."

Multiple answers allowed, may exceed 100%.

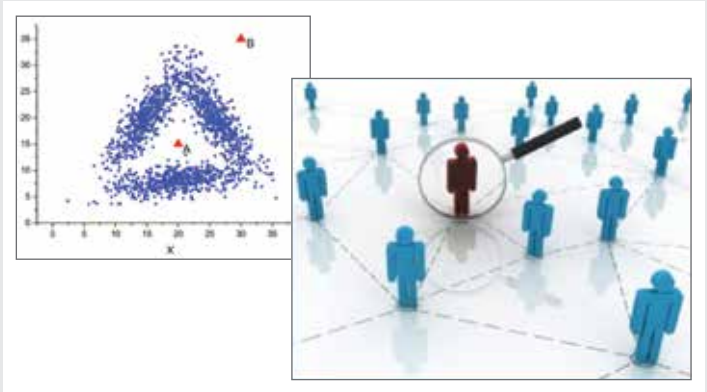
Broader FDA capabilities to help mitigate insider threat, cyber and fraud risks



Rules-based descriptive tests and reporting – By using historical data with simple and complex analytical weighted tests, significant value can be achieved to identify areas of risk. Alerts will be produced when a specific condition is met. For example, if an employee submits an expense for reimbursement with an expense amount in excess of a predefined reimbursement policy, then an alert would be triggered. These types of analytics are often easy to implement as they rely on predefined conditions and policies. For this reason, this is the most common FDA technique used by businesses.

Keyword search – The process scans free text fields and unstructured data sources to identify suspicious or high-risk language used. Companies can develop their own library of high-risk terms that incorporates industry and company-specific jargons, acronyms and cultural slangs that might be used within the specific group being analyzed. The process can be developed to take into account industry-specific terms, multiple languages and historical events so that suspicious language can be tagged and escalated for further review.

Topic modeling and linguistic analysis – These tools use text analytics to identify suspicious phrases, high-risk topics or unusual patterns of behavior in the free text components of the data. Beyond keyword searching, topic modeling seeks to cluster, quantify and group the key noun or noun phrases in the data, enabling the investigative team to quickly gain an understanding of what information may have been compromised or the corrupt intent of certain business activities. Linguistic analysis techniques use the results of text analytics to identify the emotive tone of the communication – identifying angry, frustrated, secretive, harassing or confused communications, among other sentiments.



Statistical analysis and machine learning – This technique leverages historical facts in the data and machine learning to make predictions about future or otherwise unknown events. The incorporation of statistical models into this approach further increases the confidence that items identified as outliers warrant additional review, thus limiting the amount of false positives and increasing the efficiency of the review process.

Data visualization: dashboards – Dashboards can be very powerful in the identification of unknown events. Data visualization, including heat maps, geospatial analysis, time series analysis, word clouds, stratification and drill-down techniques, enables the identification of trends and outliers in one, easy-to-understand interface. By combining transactions scoring, dashboards can aggregate threats across multiple criteria and data sources to prioritize the review.

Data visualization: pattern and link analysis – This technique provides insights, hidden patterns and relationships from vast, seemingly unrelated data sources. Data, both structured and unstructured, is provided in a variety of visual and link formats that can be used to connect one data source to another, exposing hidden relationships.

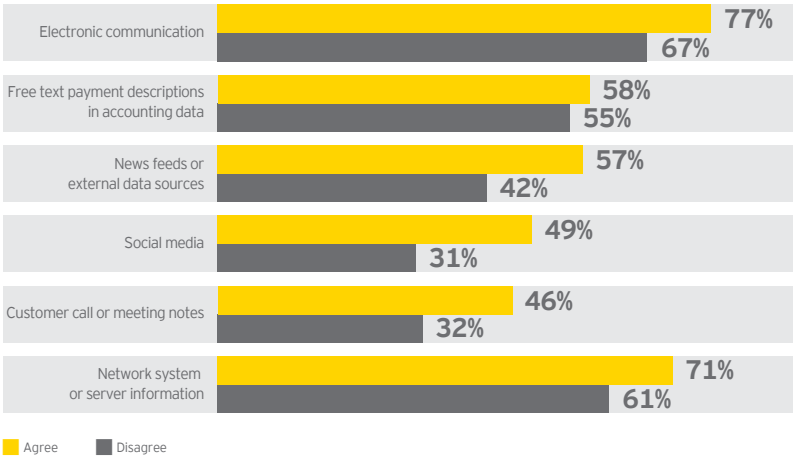
"We are seeing companies broadening their forensic data analytics capabilities beyond traditional anti-fraud and compliance functions into areas such as legal, information governance and cybersecurity."

Todd Marlin, Principal, Forensic Technology & Discovery Services, FIDS US, EY

03 Analyze a wide variety of data

Those seeing positive results are also analyzing a wider variety of data from both structured and unstructured data sources. Our survey findings indicate that respondents who have reported positive results from using FDA are using a wider variety of data sources. This offers another avenue for companies with low-volume data to leverage FDA more effectively: broadening the data sources they analyze could make their analytics more effective.

Figure 14: Use of unstructured data sources to analyze risk



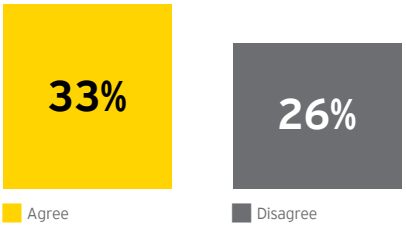
Q. Which of the above unstructured data sources does your organization use to analyze fraud risks?
Base: Among all respondents (665), 56% (370) agree and 21% (140) disagree that "We currently get positive results from the FDA tools that we use."

Multiple answers allowed, may exceed 100%.

04 Invest more of their total anti-fraud spend in FDA

Those who spend a larger portion of their anti-fraud program budget on FDA have reported a higher success rate in seeing the positive results of FDA. Those agreeing with the positive results statement spend 33% of their total anti-fraud program budget on FDA; those disagreeing spend only 26%.

Figure 15: Anti-fraud program spend in FDA



Q. Of your annual spend on preventing and detecting fraud risks, what percentage is on FDA specifically?
Base: Among all respondents (665), 56% (370) agree and 21% (140) disagree that "We currently get positive results from the FDA tools that we use."

FDA maturity model

In our 2014 survey, we introduced an FDA maturity model that provides a four-quadrant framework for assessing an FDA program's precision (i.e., its ability to better detect relevant risk issues) and accuracy (i.e., its ability to reduce the number of false positives). In that model, the most mature companies integrate all four quadrants of analytics capabilities into their FDA activities, adopting advanced data analytics technologies and combining structured and unstructured data.

We have since updated the model to show the progression of an organization's FDA maturity journey starting from rules-based, descriptive tests and reports, through keyword searching, data visualization, topic modeling and linguistic analysis, to statistical and predictive techniques. The model still suggests that as multiple analytics techniques are incorporated, the fraud detection rate increases and the false positive rate decreases. It also highlights the importance of considering both structured and unstructured data sources as indicated by the yellow arrows, regardless of the techniques being used.

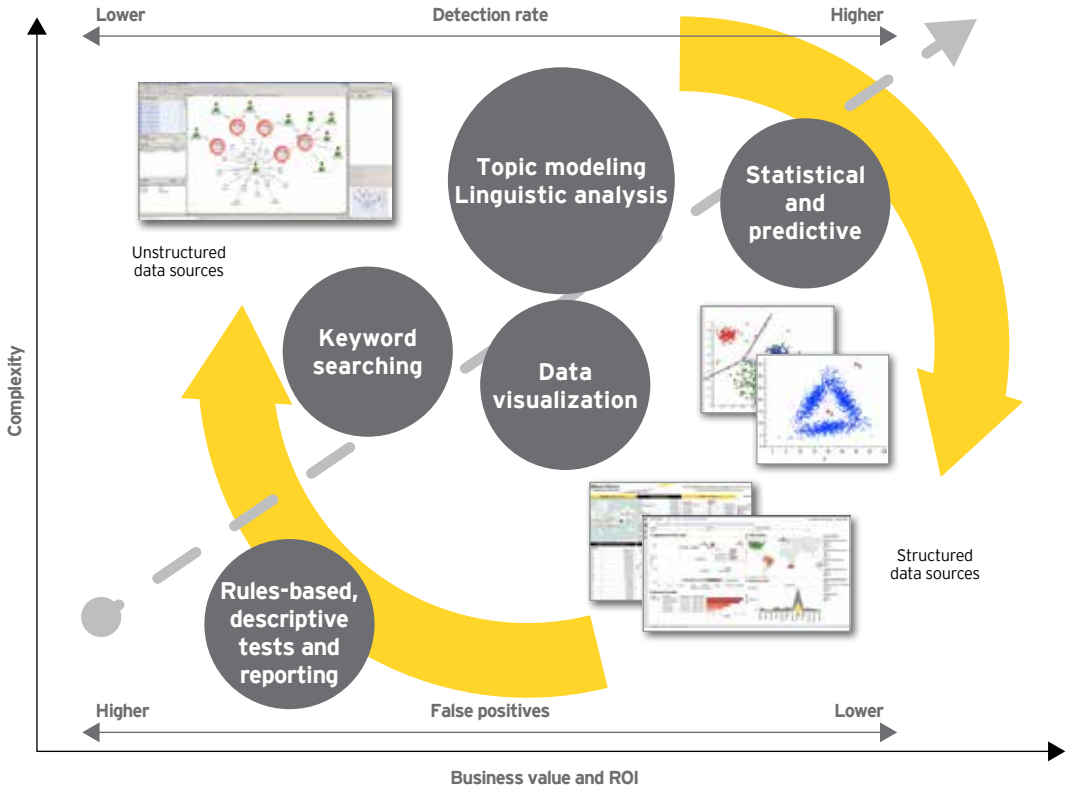
Our survey revealed that, overall, companies have increased their FDA maturity since 2014. The vast majority of companies are adopting more advanced tools. Statistical use cases rose 7%; the use of unstructured data sources rose 8%. Of note, within unstructured data sources, the highest growth category was the use of email, up 16% from 57% to 73%, while the use of call log and phone data more than doubled from 20% to 41%. Finally, the use of visualization tools also more than doubled, with one in four respondents now using these advanced tools.

Our 2016 survey findings reinforced the validity of our maturity model. In almost every circumstance, those companies using more sophisticated analytics beyond rules-based tests report better fraud detection in less time as compared with those using only rules-based tests.

> "We have to bring innovative and effective technology to eliminate or curtail money laundering or cybercrime, as well as to achieve more transparency."
>
> **CFO, Retail and Wholesale, India**

> "When combined with industry knowledge and investigative experience, insights gained from the use of leading forensic data analytics techniques can get clients faster answers to key business issues."
>
> **Jim McCurry, Partner, EMEIA FIDS Leader, EY UK**

Figure 16: Data analytics maturity journey



Case studies

Responding to a major cyber breach – theft of confidential customer information

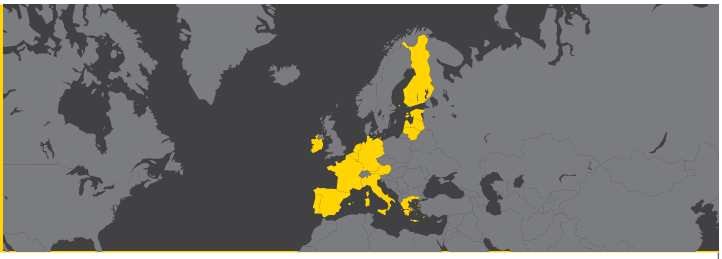
Industry: **Retail**
Country: **United States**

The situation:
The company's information systems were hacked by external actors, resulting in the loss of confidential customer information.

How FDA helped:
The company used FDA to assess the scope of the breach and its potential impact on financial systems. It conducted a forensic investigation and analysis of financial systems at the operating system, database and network layers, as well as of log data from a variety of sources, to assess the reliability of the financial controls. The company was able to confirm the integrity of its financial IT system despite the deficiency in logical access controls. The deficiency in logical access controls was subsequently remediated.

Responding to a cyber attack – account takeover and redirect

Industry: **Internet service provider**
Country: **Eurozone**



The situation:
A large European top-level domain name registrar reported that the domain names for major international companies had been hijacked and redirected to inappropriate internet sites.

How FDA helped:
The company used FDA techniques to isolate the intrusion mechanism and to evaluate the network infrastructure to determine if the intrusion had gone beyond the initial attack vector. Using pattern and link analysis to visualize network traffic, the investigation team determined that the intrusion was indeed limited in scope, which the company was able to demonstrate to regulators. The analyses provided substantive evidence that the intrusion was limited in scope, causing minimal damage to the company.

Detecting bank deposit fraud

Industry: **Banking**
Country: **Asia**

The situation:
A large Asian bank was seeking to uncover bank deposit fraud patterns across its retail business in order to improve its internal controls environment and build trust with customers and employees.

How FDA helped:
The company used advanced FDA techniques to harness data never before extracted from its core banking system, which was linked with data from other business units, such as branch and internet banking. Several billion bank transactions were loaded into a network of high-performance computers on-site. The bank developed customized counter-fraud risk-scoring models leveraging visual analytics, link analysis, statistical anomaly detection and predictive analytics techniques to spot unusual patterns of potential bank deposit fraud schemes. The bank uncovered hidden relationships between its customers and employees, highlighted suspicious insider activities and detected transactions that were designed to avoid internal reporting thresholds. The bank put together a fraud task force to review case observations resulting from the models and validated that the reduction in false positives had significantly improved.

Surveillance monitoring: Know Your Trader (KYT)

Industry: **Financial services**
Country: **Australia**

The situation:
The bank was investigating concerns raised by an Australian regulator with respect to various FX and financial benchmark processes. Specifically, the regulator issued a series of compulsory notices to the bank requiring it to produce certain documents and information.

How FDA helped:
The bank deployed KYT forensic data analysis techniques spanning more than 10 million documents – covering corporate email, instant messaging, and Reuters and Bloomberg Chat data – to identify potentially high-risk communications between the bank's securities traders, industry analysts and other parties. By using FDA, the project team performed targeted document review by applying:

- A series of keywords and ontologies designed to detect rogue trading and noncompliance with bank regulations
- A communication risk-scoring model that assigns an agreed weight to each test and ranks each communication based on the co-occurrence of how that communication meets each test criterion

By using FDA to enable a targeted document review based on text mining and an objective risk-scoring model, the number of documents requiring review was substantially reduced – cutting costs by millions, with a better risk mitigation outcome.

Embracing the FDA revolution: going the distance

The rapidly evolving digital world is seeing more and more new risks for companies to evaluate, manage and mitigate. As a result, regulators are employing more tools to detect noncompliance and working across borders to prosecute offenders. This environment has alerted boardrooms to the need to manage their risk much more effectively than before.

Companies recognize their vulnerabilities, and many more are using technology and tools, particularly around visualization, to extract more from their data. In-house capabilities are increasing, but so are outsourced services. Yet firms are failing to appreciate the full value of FDA technologies, commit to them and reap their benefits.

One major reason for FDA tools being less effective than they could be is the lack of investment. Although the C-suite is aware of the need for these tools, many companies do not invest enough in the right technology or the right skill sets to follow through and close the loop.

The signals are clear. Companies that have benefited greatly from their FDA investment use advanced technology to analyze both large volumes and a wide variety of data. They invest more of their total risk management and investigative spend in FDA.

Many organizations have already taken steps to monitor risks proactively. They have in place systems to monitor, detect and combat risks, rather than merely react to allegations and crises. Still, 37% of the respondents spend more than half of their FDA investment on reactive matters. We believe these organizations should consider investing more in proactive measures that can result in better risk management up front and reduce potential cost from fraudulent activities or noncompliance in the long run.

Emerging markets are showing awareness of cybercrime, but they have not committed as many resources to combating it as their counterparts in developed markets. Lack of funding appears to be a major constraint, but this also leaves companies at increased risk of an attack.

The final picture of FDA in 2016 is of a technology that is slowly gaining traction and beginning to yield returns on investment. But companies have not yet thrown their full weight behind the paradigm, choosing instead to invest piecemeal and reap only some of the benefits. In order to leverage the full power of FDA, firms need to commit, invest and implement the strategy in its entirety. In doing so, they will join those that are already riding the crest of the analytics revolution.

> "We need to provide better technical training to our people and improve the quality of information in our corporate systems and applications."
>
> **Risk Executive, Life Sciences, Brazil**

37%

of the respondents spend more than half of their FDA investment on reactive matters.

Survey approach

Between June and September 2015, researchers from Longitude Research, a business-to-business research and content agency, conducted 665 interviews across 17 countries with organizations actively using FDA. Respondents had to be the decision-makers responsible for their company's anti-fraud program. A breakdown of these survey respondents is as follows:

Job title	Interviews
Head of internal audit/CRO	192
Other audit/risk	81
Other finance	51
Head of compliance	61
CFO/FD	68
Head of legal	34
Financial controller	58
CEO/COO/CIO	28
Head of business unit/division	16
Head of investigations	14
Head of security	17
Company secretary	5
Other management staff	40

Industry	Interviews
Financial services	162
Consumer products, retail and wholesale	149
Life sciences	59
Oil and gas	62
Power and utilities	41
Transportation	24
Manufacturing	62
Mining	27
Technology, communications and entertainment	77
Other	2

Revenue	Interviews
More than US$5b	182
US$1b–US$5b	225
US$500m–US$1b	63
US$100m–US$500m	195

Geographic location	Interviews
Australia	40
Brazil	40
China (including Hong Kong SAR)	40
France	40
Germany	40
India	40
Ireland	40
Italy	40
Japan	40
Mexico	40
Singapore	40
Middle East (UAE and Saudi Arabia)	40
South Africa	40
Switzerland	40
UK	40
US	65

Contact information

The following EY FIDS professionals contributed to this research and are available for comments:

Contacts

David Stulb
Global FIDS Leader
+44 20 7951 2456

David Remnitz
Global FIDS FTDS Leader
+1 212 773 1311

Area FIDS Leaders

Americas
Brian Loughman
+1 212 773 5343

EMEIA
Jim McCurry
+44 20 7951 5386

Asia-Pacific
Chris Fordham
+852 2846 9008

India
Arpinder Singh
+91 22 4443 0330

Japan
Ken Arahari
+81 3 3503 1100

FIDS subject-matter resources

Australia
Warren Dunn
+61 411 755 595

Brazil
Marlon Jabbur
+55 11 2573 3554

China
Chi Chen
+86 21 22284361

France
Olivier Mesnard
+33 1 46 93 67 62

Germany
Anita Kyung-Hee Kim-Reinartz
+49 211 9352 16812

Stefan Schaffer
+49 619 6996 23595

Hong Kong
Eric Young
+852 2629 3166

Jack Jia
+852 2846 9002

India
Mukul Shrivastava
+91 22 6192 2777

Amit Jaju
+91 22 6192 0232

Ireland
Eoin O'Reilly
+353 1 2212 698

Italy
Fabrizio Santaloia
+39 02 8066 9733

Luca Marzegalli
+39 335 6653345

Japan
Ken Arahari
+81 3 3503 1100

Ichiro Sugiyama
+81 3 3503 1100

Middle East
Mike Adlem
+971 4701 0524

Paul Marsters
+971 4332 4000

Mexico
Ignacio Cortes Castan
+52 55 5283 1300

Singapore
Reuben Khoo
+65 6309 8099

South Africa
Charles R De Chermont
+27 11 502 0426

Lance Poon
+27 11 772 4207

Switzerland
Paul Wang
+41 58 286 5826

United Kingdom
Paul Walker
+44 20 7951 6935

Carl Judge
+44 20 7760 9347

United States
Todd Marlin
+1 212 773 7709

Vincent Walden
+1 212 773 3643

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the industry sector. With our more than 4,200 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.

1512-1788039
SCORE No. AU3666

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/fids