KNOWLEDGE – International Journal
Vol.31.5
June, 2019

REVEALING THE TRUE COST OF FINANCIAL CRIME, FOCUS ON EUROPE

Gramos Begolli
D.A. Tsenov Economic Acadamy, Svishtov, Bulgaria, begolli.gramos@gmail.com

Abstract: In March 2018, Refinitiv commissioned a global survey to better understand the true cost of financial crime and to raise awareness of its wider impact on business, individuals and society as a whole.
In total, over 2,300 senior managers from large organizations across 19 countries participated.
We also supplemented the survey findings by conducting in-depth research and holding interviews with leading NGOs (Education Endowment Foundation, Transparency International UK and Walk Free Foundation) and the European Union's law enforcement agency to gain perspective on the human cost of financial crime.
This report specifically examines the findings in Europe.
Keywords: Financial crime, Fraud, Companies, Risk, Organisations.

ABOUT THE SURVEY

For purposes of this report we have used a wide definition of financial crime, one that goes beyond the scope with which Refinitiv is traditionally associated. In order to provide as complete a picture as possible on the social and financial impact of financial crime, we have included bribery and corruption; money laundering; fraud; theft; cybercrime; and slave labor/ human trafficking . A total of 2,373 C-suite/senior management in large organizations across 19 countries1 completed the survey. Respondents' feedback was grouped according to the regions in which their companies operate in order to deliver a global opinion of those regions, based on first-hand experience and knowledge.
This report includes statistics covering Western Europe, Eastern Europe and Western/Central Asia. The survey sought feedback from both publicly listed and privately owned organizations.A range of industries was consulted, including agriculture; mining; construction; retail; manufacturing and financial. Please note that the standard convention of rounding has been applied and consequently some totals do not add up to 100%.

THE HIDDEN FACE OF FINANCIAL CRIME

The true cost of financial crime extends far beyond pure economics.
Critical social consequences include the proceeds of financial crime being used to fund the financing of terrorism; human rights abuses such as slavery and child labor; and environmental crime. Loss of revenue to national governments has a host of knock-on effects, too, including the fact that lower tax revenues mean that less money is available to fund schools, hospitals and other essential services. On a macro level, raising awareness is a key tool, as is collaboration and the sharing of information and ideas on the best methods to combat financial crime.
On an organizational level, invaluable tools include access to reliable risk data that offers breadth of risk intelligence coverage and finding the right partners to enable a holistic approach to effective risk mitigation throughout the compliance process. Financial crime affects everyone and gaining insight into its true magnitude and devastating effects is of paramount importance.
Financial crime: some background to the challenge

EXTENSIVE NETWORKS

One of the ways in which financial crime can flourish is to 'hide' in organizations' third-party networks that are often extensive and can span the globe. To better understand themagnitude of these networks, our survey asked respondents to estimate how many third-party vendor, supplier or partner relationships their company had, globally, over the 12 months preceding the survey. The average across the globe was reported as 7,693 such relationships,against a proportionately higher number in Western Europe of 8,591 and an even higher number – 10,207 – in Eastern Europe and Western/Central Asia.

EVER-INCREASING PRESSURE

Organizations are operating against a backdrop of growing pressure – pressure to increase turnover, grow profits, develop new markets, increase market share and improve regulatorysafeguards. When asked how they would generally rate the pressure upon their companies to achieve in these areas in the 12 months postsurvey, 83% across the globe reported that pressure to increase turnover is either extreme or significant. The same pressure was evident

across Europe, with 82% in Western Europe and 83% in Eastern Europe and Western/Central Asia also citing pressure to increase turnover. [181]

INITIAL SCREENING AND ONGOING MONITORING

This pressure, added to a host of global regulations and legislation to combat financial crime, has led to a situation where compliance teams often struggle to fully screen and monitorthe vast number of customers, thirdparty vendors, suppliers and partners identified above.

The consequences of compliance failure are significant and compliance teams are aware of their responsibilities, but nonetheless often struggle with the task at hand. Across the globe, respondents revealed that an average of just 59% of global customers, third-party vendors,suppliers or partner relationships were ever screened with regard to financial crime issues, including bribery and corruption; money laundering; fraud; theft; cybercrime; and slave labor/human trafficking.

In Western Europe, this figure drops to 58% (the lowest percentage across all regions surveyed), but rises slightly to 60% across Eastern Europe and Western/Central Asia.We then asked respondents what percentage of those initially screened are monitored and reviewed on at least an annual basis. The global average was once again 59%, but lower in both Western Europe (57%) and Eastern Europe and Western/Central Asia (58%). This means that only about a third of relationships are fully screened (initially and on an ongoing basis) across the region.

MEASURING THE IMPACT OF FINANCIAL CRIME

Survey responses indicate that large percentages of companies have been victims of some form of financial crime within their global operations during the 12 months preceding the survey. Globally, 47% had been a victim of at least one form, with Eastern Europe and Western/Central Asia on par and slightly higher numbers reported in Western Europe at 49%.

The true cost of such crimes must be measured in terms of their financial, social and humanitarian impact. Within each country surveyed, we calculated the sum of the published turnover (last 12 months) of listed companies with a turnover of USD$50 million or more and applied a global estimate of lost turnover as a consequence of financial crime at 3.5%, giving a global estimated loss of turnover of just over USD$1.45 trillion. On the same basis, we analyzed 2,376 listed companies in Europe with a total sum turnover USD$9.9 trillion and the estimated loss amounted to USD$319 billion. In concrete terms, what could this lost revenue have meant? By way of example, let's look at how much $1 billion can buy in the vital area of education in different countries across the globe. In Spain, this amount could pay for highquality early years education for 150,000 toddlers, whilst in Russia $1 billion could provide 180,000 toddlers with the foundations they need to become fluent learners at school. In Mexico, it would mean 327,000 additional children placed in primary and secondary schools; and in India $1 billion could build 2,000 more schools. In Poland, this money could pay for 64,000 additional teachers, or 21,000 in the USA. These examples just begin to illustrate the real-life consequences and impact on individual lives as a direct result of every dollar of revenue lost to financial crime.

DIFFERENT ASPECTS OF FINANCIAL CRIME

Perceived relative importance

What aspects of financial crime do organizations feel are the most important to prevent?

In every region surveyed, the lowest percentage of respondents considered slave labour/human trafficking to be important, suggesting a widespread lack of appreciation of the importance of addressing and eradicating these crimes against humanity. With an estimated 40 million people living in modern slavery, the human and economic costs are enormous.

A 2014 report by the International Labour Office (ILO) puts the cost at $150 billion. It is likely that the real numbers are far higher. Conversely, two areas – bribery and corruption; and cybercrime – stood out across all regions, with the highest percentage across the globe (94%) selecting bribery and corruption as an important issue to tackle.

Within Europe, 93% of respondents in Western Europe indicated that both bribery andcorruption and cybercrime are important aspects to tackle, whilst in Eastern Europe and Western/Central Asia bribery and corruption was selected by 94% of respondents. In the 12 months preceding the survey,the percentage of turnover lost to bribery and

[181] Revealing the true cost of financial crime Focus on Europe, Didier Lavion Principal, Global Economic Crime andFraud Survey Leader, PwC US.

corruption was an average of 3.1% in Western Europe and 3.5% in Eastern Europe and Western/Central Asia. The global average was 3.2%. In Western Europe 56% believe that the consequence of this bribery and corruption will be higher prices for end users, a view echoed by 57% of respondents in Eastern Europe and Western/Central Asia. 90% in Western Europe and 91% in Eastern Europe and Western/Central Asia agreed (either strongly or slightly) with the statement 'we struggle to educate and influence colleagues on bribery and corruption in some regions'.

THE CURRENT STATE OF PLAY - How much are companies spending?

As a percentage of global turnover, how much did companies spend to prevent financial crime issues around their global operations during the 12 months preceding the survey? Responses indicate that this figure is 3.1% across the globe; slightly lower at 2.9% (the lowest percentage across all regions surveyed) across Western Europe and 3.2% across Eastern Europe and Western/Central Asia.

Shortcomings in formal compliance

Respondents were further asked how well their companies presently undertake a range of formal compliance procedures in relation to customers, third-party vendors, suppliers or partner relationships.

The list included:

- Screening and classifying risk
- Conducting due diligence
- Monitoring and refreshing
- Implementing workflow and process reports
- Training and educating

Shortcomings were evident, with respondents globally revealing that just 57% fully screen and classify risk; 52% fully conduct due diligence; and 52% fully monitor and refresh records. Within the region, some notable gaps were also evident, as follows:

- In Western Europe under half (49%) fully monitor and refresh; and the same percentage fully implementworkflow and process reports
- In Eastern Europe and Western/ Central Asia 54% fully monitor and refresh; and the same percentageimplement workflow and process reports Even though companies across Europe are spending in the region of 3% of their global turnover to fight financial crime, significant gaps in compliance procedures remain.

TRAINING GAPS

Gaps in training across all the subsections of financial crime covered in this report were revealed bysurvey respondents and suggest an opportunity for organizations going forward. For example, globally, just 46% confirmed that formal training is undertaken by colleagues in identifying, preventing and reporting breaches in slave labor/human trafficking, meaning that over half of global respondents' organizations either don't undertake training in this important area, or they don't know that they do, raising another important issue – one of awareness.

Within Europe under half – 46% in Western Europe and 49% in Eastern Europe and Western/Central Asia – confirmed that formal training in this regard is undertaken. A lack of training in this area was evident within every region surveyed.

46% Western europe.

49% Eastern europe and western central asia confirmed that formaltraining is undertaken by colleagues around the globe in identifying, preventing and reporting breaches in slave labor/human trafficking.

FINDING SOLUTIONS - THE IMPORTANCE OF DATA

When it comes to rooting out financial crime, reliable and complete data is a critical requirement needed to develop a 360 degree view of risk.

Additional Refinitiv research has revealed a plethora of challenges that organizations encounter, specifically relating to third-party risk data. These include unreliable risk data sources, insufficient availability of risk data and poorly connected data sources. Respondents were asked what they consider most valuable when selecting a financial crime data vendor, including advanced technology capabilities; subject matter expertise; research methodology; and breadth and depth of information.

Respondents across all regions overwhelmingly (95% or above) either already have or would consider a vendor with all of these attributes.

COLLABORATION AS A TOOL TO FIGHT FINANCIAL CRIME

Tools to fight financial crime

Refinitiv offers a holistic approach to help businesses identify, mitigate and act upon the risk associated withfinancial crime. Our broad range of solutions encompasses:

- Risk intelligence screening
- Screening as a managed service
- Geopolitical risk ranking
- Enhanced due diligence
- Transaction monitoring

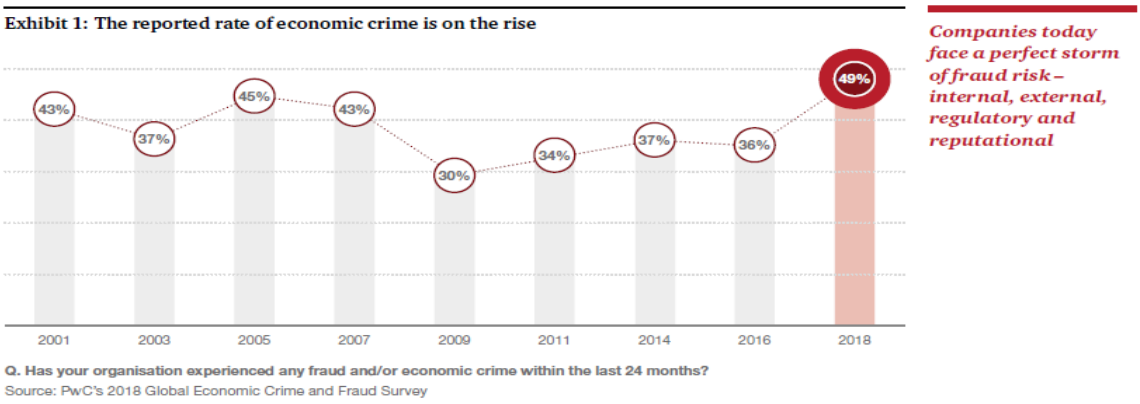
We provide a centralized, scalable and integrated suite of solutions, powered by World-Check, the trusted andaccurate source of risk intelligence.

Four steps to fight fraud:

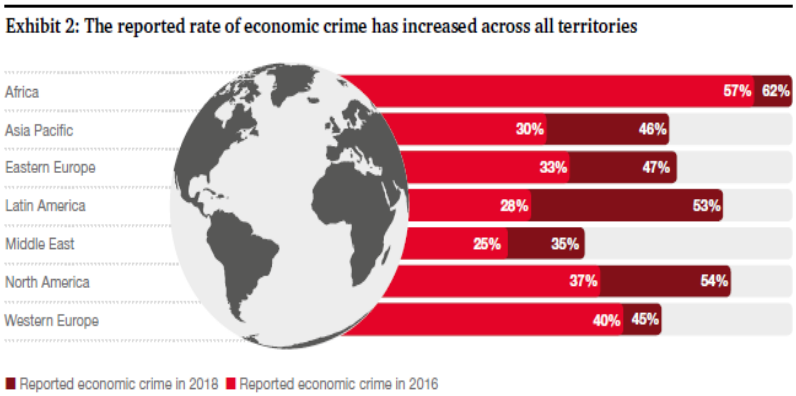
1.Recognise fraud when you see it
2.Take a dynamic approach
3.Harness the protective power of technology
4.Invest in people, not just machines

RECOGNISE FRAUD WHEN YOU SEE IT - Is fraud really on the rise – or just our awareness of it?

This year, 49% of respondents to our Global Economic Crime and Fraud Survey said their companies had been victims of fraud or economic crime, up from 36% in 2016. This rise can be explained by a combination of growing globalawareness of fraud, a larger number of survey responses, and greater clarity about what 'fraud' actually means. But every organisation – no matter how vigilant – is vulnerable to blind spots. And because those blind spots usually only becomeapparent with hindsight, throwing light onto them as early as possible can vastly enhance raudfighting efforts.



Companies today face a perfect storm of fraud risk – internal, external, regulatory and reputational



Just as the reported rate of economic crime has increased since 2016, so has the amount that companies are spending to fight it: [182]

• 42% of respondents said their companies had increased spending on combatting fraud and economic crime over the past two years (up from 39% in 2016).

• 44% of respondents said they plan to boost spending over the next two years.

Where is this money being spent? Organisations are using ever-more powerful technology and data analytics tools to fight fraud. And, in addition to these technology-based controls, many are alsoexpanding whistle-blower programmes and taking steps to keep leadership in the loop.

But do these measures represent a genuine shift to more proactive approaches to fraud and corruption? Or are they just a rear-guard action, driven principally by enhanced anti-bribery/anticorruption legislation and increasingly globalised forms of enforcement? In other words, are we still missing something vital in the fight against fraud? Our survey results strongly suggest we are.

CONDUCT RISK: THE 'HIDDEN RISK' BEHIND MANY INTERNAL FRAUDS

Two types of fraud – consumer fraud and business misconduct – have grown in prominence to such an extent that this year's survey is measuring them as separate threats for the first time. Of the respondents who indicated their companies had experienced fraud in the last two years, 29% said they had suffered from consumer fraud and 28% said they had suffered from business misconduct (making these, respectively, the 3rd and 4th most frequently reported frauds this year, behind asset misappropriation at 45% and cybercrime at 31%).

It should be noted that the significant decrease in reported incidents of asset misappropriation (down from 64% in 2016) is at least partly explained by the inclusion of these new frauds in the survey. These methodological changes reflect the growingrecognition of a broad category of internal fraud risk: "conduct risk". This is the risk that employee actions will imperil the delivery of fair customer outcomes or market integrity. And, unlike operational breakdowns or external threats (whichcan often be checked by internal controls), conduct risk requires a more holistic response – and a shift in attitude.

LOOKING FOR FRAUD IN THE RIGHT PLACES

Our survey revealed a significant increase in the share of economic crime committed by internal actors (from 46% in 2016 to 52% in 2018)and a dramatic increase in the proportion of those crimes attributed to senior management (from 16% in 2016 to 24% in 2018). Indeed, internal actors were a third more likely than external actors to be the perpetrators of the mostdisruptive frauds. However, one of a company's biggest fraud blind spots – and biggest threats – is often not to dowith its employees, but rather the people it does business with.

These are the third parties with whom companies have regular and profitable relationships: agents, vendors, shared service providers and customers. In other words, the people and organisations with whom a certain degree of mutual trust is expected, but who may actually be stealing from the company.

TAKE A DYNAMIC APPROACH

Chief executives are accountable

Our survey underscores that the direct monetary cost of fraud and its aftermath can be substantial. But when secondary costs (such as investigations and other interventions) are included, the true picture of overall cost can be much higher.

46% of respondents said their organisation spent the same or more on investigations and other interventions than was directly lost to fraud itself.

When the financial costs of fraud hit the bottom line of a business, it is only natural for the board and shareholders to require explanations from senior management. In today's world, however, a leader's responsibility doesn't stop there. In fact, that's justthe beginning.

HARNESS THE PROTECTIVE POWER OF TECHNOLOGY

Finding the technology sweet spot

When it comes to fraud, technology is a doubleedged sword. It is both a potential threat and a potential protector. Thus, as companies come to view fraud as first and foremost a business problem which could seriously hamper

[182] **Didier Lavion** Principal, Global Economic Crime and Fraud Survey Leader, PwC USSource: PwC's 2018 Global Economic Crime and Fraud Survey,

growth, many have made a strategic shift in their approach to technology. These companies are making a business case for robust new investments in areas such as detection, authentication and the reduction of customer friction.

Today, organisations have access to a wealth of innovative and sophisticated technologies with which to defend themselves against fraud, aimed at monitoring, analysing, learning and predicting human behaviour. These include machine learning, predictive analytics and other artificial intelligence techniques. And our survey shows companies are using these technologies, to varying degrees, depending on the industry sector. Technology is expensive to buy and to adopt across a large organisation – prohibitively so, for some.

INVEST IN PEOPLE, NOT JUST MACHINES

A small investment in people can pay huge dividends

Confronted with the seeming intractability of dealing with fraud, many organisations decide to pour ever more resources into technology. Yet these investments invariably reach a point of diminishing returns, particularly in combatting internal fraud.

So, while technology is clearly a vital tool in the fight against fraud, it can only ever be part of the solution. This is because fraud is the result of a complex mix of conditions and human motivations. The most critical factor in a decision to commit fraudis ultimately human behaviour – and this offers the best opportunity for combatting it. There is a powerful method for understanding and preventing the three principal drivers of internal fraud – the fraud triangle.

CONCLUSION

Our survey shows that many companies are underprepared to face fraud, for both internal and external reasons. This is why shining a light on an organisation's fraud blind spots, and sharing a clear understanding of what constitutes fraud – and what needs to be done to prevent it – is so important. Doing so can also unlock significant opportunities. It can help make positive structural improvements across the organisation – which can make the business stronger and more strategic in both goodtimes and bad. That includes removing siloes in functions like compliance, ethics, risk management and legal – and enabling a culture that is more positive, cohesive and resilient. It's true that the value proposition of an up-to-date fraud programme can be hard to quantify, making it sometimes difficult to secure the investments needed. But the opportunity cost – financial, legal,regulatory and reputational – of failing to establish a culture of compliance and transparency can be far greater.

LITERATURE

Didier Lavion Principal, Global ,Economic Crime and Fraud Survey Leader, PwC USRevealing the true cost of financial crime Focus on Europe

Didier Lavion Principal, GlobalEconomic Crime and Fraud Survey Leader, PwC USSource: PwC's 2018 Global Economic Crime and Fraud Survey

Rieley J.B. & Clarkson I., 2001

L.Greiner 2001