Time to change tack

A need for new thinking by the Financial Services industry

53%
of Financial Services respondents increased spending on compliance over the last 24 months

46%
have suffered economic crime in the last 24 months

35%
stated that economic crime had high or medium impact on relationships with regulators

29%
of economic crimes in Financial Services organisations were committed by internal perpetrators

pwc

www.pwc.com/crimesurvey-fs

Overview

We have been performing a global survey of economic crime since 2001, and despite significantly increasing investment in compliance and being continuously under the scrutiny of regulators in that time, 46% of respondents in the Financial Services industry reported being victims of economic crime in the last 24 months, an increase from 45% reported in 2014.

Our Financial Services insights combines results for the Banking & Capital Markets and Insurance sectors. It remains difficult for Financial Services organisations to join the strategic dots across the growing volume, sophistication and variety of economic crime. 16% of those that reported experiencing economic crime had suffered more than 100 incidents, with 6% suffering more than 1,000. Not only are the direct losses from these incidents higher than in other sectors, but in the regulated world, it is the costs of remediation and compliance that are staggering.

Tackling economic crime and proving positive intent to regulators has often meant more spending on compliance. 53% of respondents reported that spending on fighting economic crime was increasing – a trajectory that shows no sign of stopping. However, spending significantly more has not meant less economic crime. Our survey found that Financial Services organisations place more value on relations with regulators than any other group – including their employees and business partners. But this focus and investment has failed to deliver better relationships with 50% of respondents having undergone regulatory inspections or experienced enforcement action in the last 24 months.

Even if further spending could deliver better relationships and results – Financial Services also faces a global shortage of sufficiently skilled and experienced compliance professionals, particularly in areas such as Anti-Money Laundering and Counter-Terrorist Financing ('AML-CFT') compliance, to help understand and manage the interconnected risks of economic crime. So what is the answer? Our advice to Financial Services organisations is to focus on efficiency and effectiveness, not just activity.

Spending should be targeted where it can make the biggest difference. For sophisticated global institutions, this means automating labour-intensive processes, improving the quality and accessibility of information and evaluating new, more effective technological detection methods. 33% of our respondents revealed that data quality still can restrict compliance with anti-money laundering regulations. Financial Services organisations need strategic financial crime risk assessment frameworks to make sure policies and compliance programmes target the areas of greatest risk. And the best way to tackle financial crime is by embedding the latest strategies and technology into day-to-day operational decision making. And, to combat the stark fact that 29% of economic crime is committed by internal perpetrators, organisations must also continue to invest in creating corporate cultures based upon strong shared purpose and values.

New thinking is needed to make investment in compliance deliver more value and to tackle economic crime.

Change in compliance spending in next 24 months

18% of respondents expected significant increase in spending

37% expected some increase

39% expected spending at the same level

6% planned to reduce spending

$70.2bn New regulation stemming from the financial crisis cost the six largest US banks $70.2 billion by the end of 2013.

Up from **45%** in 2014 and **36%** global average

46% of respondents reported experiencing economic crime in the last 24 months

Investigating crime

33% stated that data quality was a significant challeng

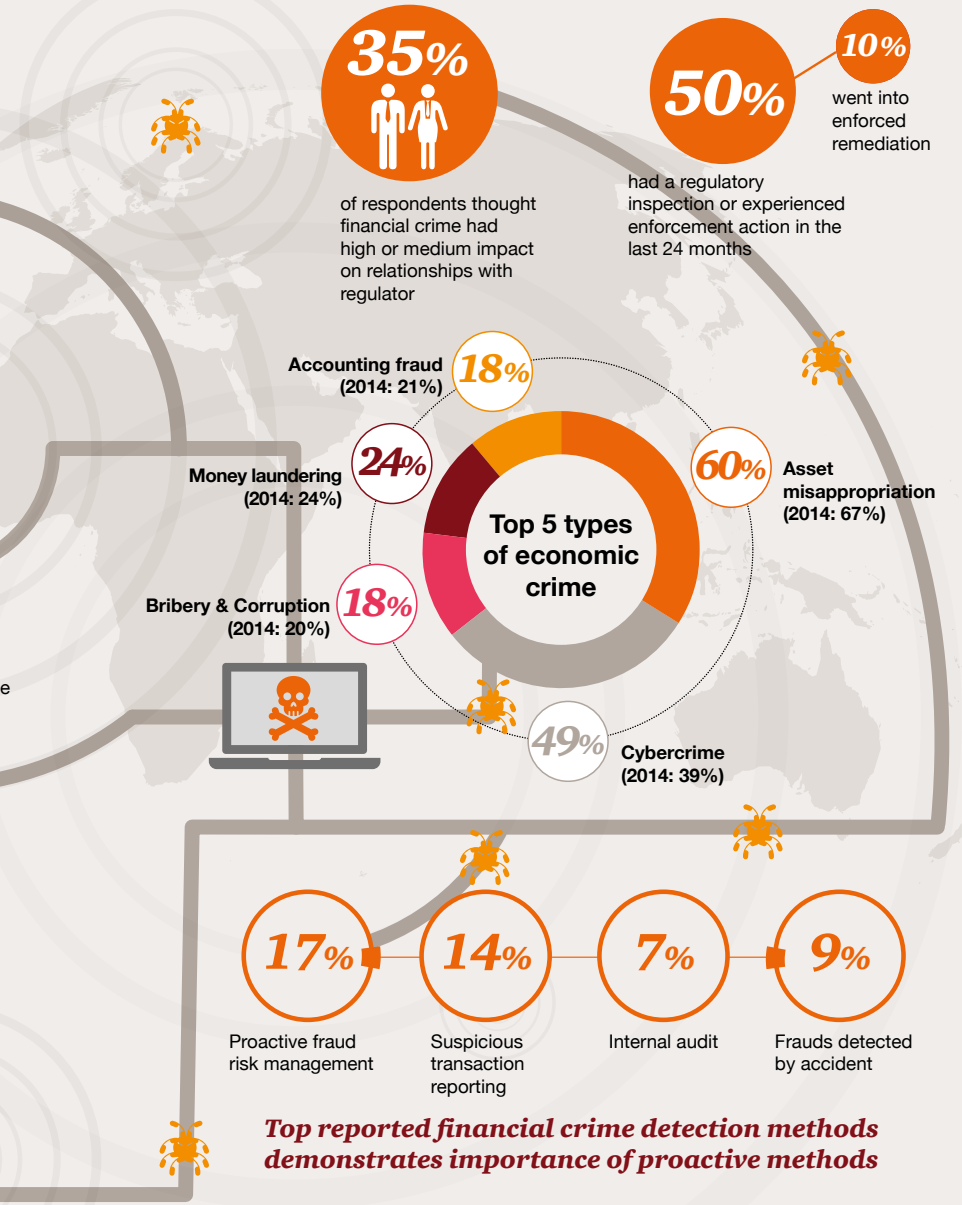
Committed fraud

58% by external perpetrators (2014: 57%)

79% of frauds were investigated internally

29% by internal perpetrators (2014: 39%)

Relationships with regulators



Top reported financial crime detection methods demonstrates importance of proactive methods

1

Compliance – cost or opportunity?

New regulation stemming from the financial crisis cost the six largest US banks $70.2 billion by the end of 2013.[1] For Financial Services organisations, navigating local and global regulations can be frustrating, difficult and is increasingly costly.

53% of Financial Services respondents reported that spending had increased over the last 24 months and 55% thought it would increase again in the next 24 months.

The pace of change puts continual pressure on organisations to embed new systems and processes and keep up with requirements. For example, 19% of respondents stated that the pace of regulatory change was a significant challenge for Anti-Money Laundering (AML).

In the UK, a recent National Audit Office report has said the Financial Conduct Authority (FCA) needs to do more to assess the cost of compliance for firms in order to understand how effective its policies were.

Making compliance data work harder

Regulatory pressures are a fact of life for Financial Services but organisations can do more to maximise the value of their compliance programs. In February 2015, *Andrew Ceresney, the SEC's Director of Enforcement*, noted that organisations "must ensure that there is communication across different aspects of the compliance program and business."[2] He noted that "one of the lessons of some of our recent cases is the importance of integrating AML compliance with other aspects of the compliance program and with the business generally."

Any innovation that gives faster insights into fraudulent activity and helps Financial Services organisations get ahead of criminal activity and maintain economic crime controls is welcome. But there is a danger that the proliferation and choice of analytical advancements has created more confusion than clarity. Questions have been raised about quality and reliability of the analytics and also if regulators have had sufficient input into their development and application.

Successful organisations will find new ways to maximise value from compliance activities and processes by:

- **Creating value –** For instance in response to feedback from regulators, the compliance department of a major financial institution was required to enhance its Know-Your-Customer (KYC) programme. A dedicated team invested months analysing accounts to identify patterns of suspicious transactions. The results helped demonstrate to the regulators that the accounts were compliant with AML regulations. However, this is not the end of the story. The financial institution took the insights into customer travel patterns and foreign transactions gained when analysing the accounts, and used the information to market products such as travel insurance and targeted credit card offers.
- **Using faster, more cost-effective reporting –** KYC checks are a huge administrative burden for Financial Services. So the promise of KYC utilities, that reduce the time, resources and operational costs of client checks, is appealing. Thinking about the most efficient process for collecting data can also provide a client dividend, as it avoids having to ask clients the same questions multiple times. But KYC utilities are not a riskless proposition – financial institutions will be using the information these utilities provide to make risk-based decisions about their clients. They need to be confident that it is reliable.
- **Leveraging new data and new insights –** Compliance teams have traditionally taken responsibility for trade and communication surveillance. Our 2016 EMEA Surveillance Survey highlights increased investment in big data techniques to trawl the millions of messages generated each day against lists of key words and phrases that may indicate suspicious behaviour. Technological innovations are providing faster insights into fraudulent activity and allowing organisations to streamline activities.

pwc

[1] Federal Financial Analytics, "The Regulatory Price-Tag: Cost Implications of Post-Crisis Regulatory Reform," July 2014
[2] https://www.sec.gov/news/speech/022515-spchc.html

Collaborative relationships with regulators

Across the Financial Services industry, economic crime not only introduces reputational risk that may damage fragile customer relationships – it also has a negative impact upon the relationships with industry regulators. 35% of respondents thought financial crime had a high or medium impact on relationships with regulators.

50% of Financial Services respondents had a regulatory inspection or experienced enforcement action in the last 24 months. 10% of those that had an inspection were placed into enforced remediation. What these figures show is that trying to demonstrate positive intent to industry regulators, through tactical compliance investments, has failed to deliver better relationships. Regulators have become more demanding – as *Reserve Bank of India Governor Raghuram Rajan* put it, a regulator cannot be a "paper tiger". [3]

Our survey shows that respondents invest more in relations with regulators than any other group – including their employees and business partners. If organisations and regulators cannot build effective relationships, there is danger that the industry will choose to limit commercial activity rather than risk falling foul of regulation – a risk the Irish regulator noted has the "potential to push certain business and customers into unregulated or less regulated channels…and may actually impede the effective implementation of AML/CFT measures." [4] New thinking from both the industry and regulators is needed. Financial Services organisations need to be more open with regulators about their weaknesses. And in a rapidly changing world, regulators need to move more quickly to replace regulations that no longer make sense. As Mexico's regulator noted, the "challenge is to maintain a dynamic regulation that fosters innovation." [5]

Regulators take an innovative and collaborative approach

AsiaPac – Development of Interpol Global Complex for Innovation (IGCI) in Singapore

- The Singaporean regulator (MAS) is collaborating with FinTech companies to develop a cutting edge research and development centre focused on finding ways to combat financial crime.
- The IGCI goes beyond the traditional reactive law enforcement model, providing proactive research into the latest threats and training organisations in proactive defence and response.
- The aim is to counter increasingly ingenious and sophisticated criminal techniques by sharing tools and capabilities with global law enforcement.
- MAS is developing new regulatory policies and strategies – using technology to manage risk, enhance efficiency and help organisations remain competitive.

How can we help?

When compliance gets personal

Regulators are seeking to introduce more personal accountability across financial services organisations. In the UK, executives are being asked to personally attest to the effectiveness of economic crime and regulatory compliance controls through the Senior Manager Regime. In the US, a prominent CCO was fined $1m for control failures and the Department of Justice's Yates Memo has made it clear that more similar action will follow. We provide support to managers of Financial Services organisations who need comfort that the controls they are responsible for are effective. We can help organisations understand whether they are lagging behind acceptable practice and put in place plans to implement necessary enhancements.

pwc

[3] http://www.thehindubusinessline.com/money-and-banking/we-cannot-be-seen-as-a-paper-tiger-raghuram-to-rbi-staff/article8055058.ece
[4] https://www.centralbank.ie/press-area/speeches%5CPages%5CAddressbyDirectorofEnforcement,DervilleRowland,tolBECSeminar.aspx
[5] http://www.thehindubusinessline.com/money-and-banking/we-cannot-be-seen-as-a-paper-tiger-raghuram-to-rbi-staff/article8055058.ece

2

Building an effective culture

Tackling economic crime in Financial Services organisations is not just about compliance — it is a question of culture. Even the most sophisticated and rigorous compliance programmes will fail if a company's culture allows or accepts wrong-doing as an acceptable way to do business. James Hubbs, Assistant Superintendent in Canada's regulatory authority, noted earlier this year that the extent of fines levied on global banks "demonstrates that misconduct is not limited to just a few bad apples".[6]

58% of frauds were committed by external perpetrators and, in Financial Services 29% were committed by internal perpetrators. Many more may have involved some degree of collusion, often unintended, between outsiders and employees.

So who are these internal fraudsters? Our survey shows that 14% of the individuals committing these acts are from layers of senior management. This raises concern over the checks and balances that exist at the top of some organisations.

Embedding a compliance culture throughout the organisation strengthens the overall control environment and can be achieved by:

- Developing a code of conduct that articulates organisational values and requirements for ethical behaviour
- Implementing a confidential escalation channel with no fear of retaliation
- Making ethical conduct a key component of employee performance and recognition
- Senior leaders demonstrating the importance of ethics
- Applying consistent disciplinary procedures for all grades
- Ensuring rewards are fair and consistently calculated

pwc

[6] http://www.osfi-bsif.gc.ca/Eng/Docs/jh20160505.pdf

Behavioural research tells us that we're less likely to be influenced by rules as we get older.[7] We are more likely to act according to our experience and the ways we've always behaved in the past. We are able to rationalise our actions based on previous outcomes – but this may not be the right thing to do. In other words, the older we get, the more willing we are to break the rules and to act according to our own personal moral compass. This is a vital insight when it comes to regulatory compliance, because it suggests that more rules are not the solution. The real answer is to strengthen and optimise the working culture through strategic alignment of corporate purpose, values and desired conduct, and thus reinforce what behaviours the organisation – and other key stakeholders expect.

Embedding an effective culture

Changing culture is difficult but it can be done. The airline and oil and gas sectors are rightly proud of their comprehensive safety cultures. These industries have demonstrated that written rules, standards and procedures, while important and necessary, were not enough and have embedded the value of safety in every level of the workforce. They have changed attitudes and behaviour. For Financial Services, embedding a compliance culture also requires a holistic approach that breaks down the siloed thinking that exists in most organisations – in this case to make connections between the risks of different types of financial crime.

The President of German Regulator BaFin, Felix Hufeld, noted that successfully tackling economic crime requires a "huge bundle of measures including, but not limited to IT investments, cultural elements and training of employees."[8]

Proactive financial crime risk management: the most effective way to counter economic crime

Proactive fraud risk management has proven to be the most effective method of detecting economic crime. It requires a strategic approach, the correct governance framework and the right information to embed fraud risk management into business-as-usual decision making. 17% of instances of economic crime were detected through proactive fraud risk management versus 14% through formal suspicious activity monitoring.

Questions to help Financial Services organisations put risk in context

- To what extent has the link between culture, behaviour and risk been made in determining exposure to financial crime?
- What measures of performance are being used to assess the level to which an effective culture is embedded through decision-making and risk management?

What is the motivation for internal fraudsters?

70% is opportunistic
These are people with the opportunity and/or ability to carry our crimes against their employers. Reducing the opportunity must be a focus for Financial Services organisations.

19% is incentive or performance pressures
This is higher than the global average and may suggest that pressure on Financial Services employees may be a risk factor.

How can we help?

Undertaking an enterprise-wide risk assessment will help organisations understand the current and potential threats and stay ahead of those with criminal intent. But more importantly, organisations need to establish a comprehensive view of risk in context for their organisations. Performing a risk assessment is not about bringing down the shutters on innovation, but balancing risk management with the need to deliver commercial success and growth. The goal for Financial Services organisations must be to understand financial crime and tackle risk head on with mitigating controls, rather than walking away from commercial opportunities. We support organisations assess financial crime threats and develop frameworks to respond to current and emerging risks. We also have the capabilities and experience of conducting enterprise-wide assessments of ethics and compliance programme effectiveness, including the use of tools to assess behavioural risk.

pwc

[7] Ethicability, Roger Steare Consulting Limited, 5th edition, 2013
[8] https://www.boersen-zeitung.de/index.php?li=1&artid=2015122005&titel=BaFin-kritisiert-die-Deutsche-Bank-oeffentlich

3

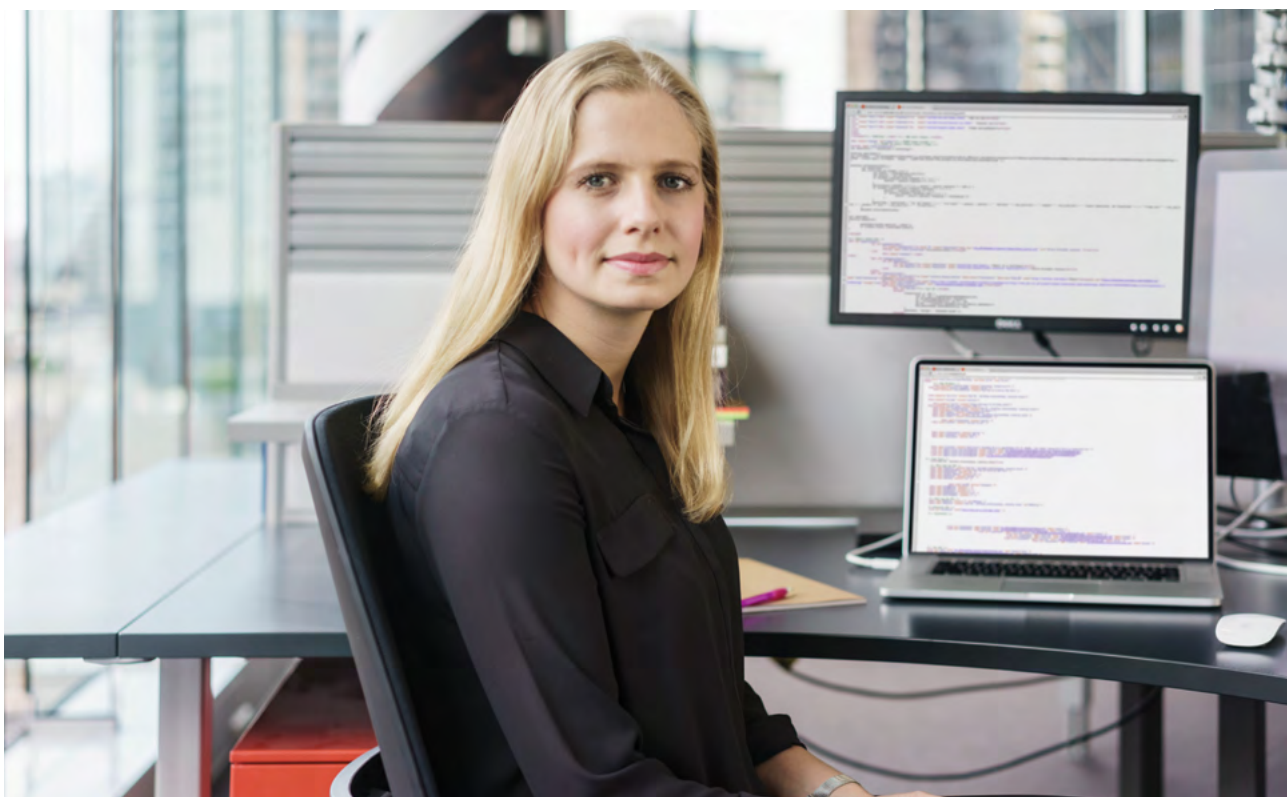
Exploiting technology to reduce economic crime and increase efficiency

Understanding, evaluating and implementing new technology solutions has never been a more critical skill. Making informed decisions about what to buy and when, helps organisations to achieve a competitive edge whilst managing risk and compliance.

Regulators have demonstrated support for new technologies and approaches. In the UK, the FCA's Project Innovate has sought to encourage the development of start-up and FinTech suppliers.

Christopher Woolard, the FCA Director of Strategy and Competition, recently noted that the "key challenge for government, industry and regulators is to continue to ensure the regulatory environment fosters the best of financial innovation." [9]

The New Zealand Financial Markets Authority recently noted that "we are looking for appropriate systems and controls, not one-size-fits-all." [10]



pwc

[9] https://www.fca.org.uk/news/uk-fintech-regulating-for-innovation
[10] https://fma.govt.nz/assets/Reports/AML-CFT-2015-annual-review-report.pdf

These are four key technologies all Financial Services organisations should be aware of in order to protect and grow their business:

Big data analytics – as well as being used to maintain real-time surveillance of the millions of messages Financial Services organisations generate each day, big data analytics is also being used to understand evolving external and internal security risks, monitor user behaviour and network activity. The risk of cybercrime now tops the list of frauds the respondents to our economic crime survey think most likely to occur in the next two years. And this concern is well placed. Some cyber professionals predict breaches that could result in 'extinction level events' costing billions of dollars and irretrievably damaging reputations. Giving information security specialists greater visibility to risk in a business context improves their capability to detect and respond to threats. Building up patterns of behaviour using techniques such as machine learning can help organisations build a predictive capability to prevent attacks before they occur.

Blockchain – Financial Services organisations are exploring how Blockchain could transform the way they trade and manage back-office operations – to name just two applications. They recognise that this technology could transform their capabilities in some areas – offering ways to process transactions more efficiently, securely, and more reliably.

Biometrics – Financial Services is built on trust and key to that trust is ensuring that people are who they say they are. To maintain trust and reduce the risk of fraud without onerous authentication processes, Financial Services organisations have commercially exploited biometrics that allow customers to access their accounts using voice and facial recognition. However, *Jin Woong-Sup, Head of the Korea Financial Supervisory Service,* has recognised there is "incredible operating and reputational risk if [banks] they fail to effectively control their customers' bio-information and imaging records." [11]

Advanced IT security – The increasing prevalence of cyber-crime also highlights the need for focus on technology that protects business integrity. 37% of Financial Services respondents stated that they were affected by cyber-crime in the last 24 months. Cyber-crime continues to facilitate and converge with other types of financial crime and organisations will increasingly need to tackle both risk together.

How can we help?

We have in-depth knowledge of regulatory guidelines and best practices for the use of technology systems to tackle economic crime. We can help to assess risk across business areas and develop monitoring process to mitigate risk. Our expertise includes:

- Holistic risk overviews to enable fact-based decision making
- Supporting technology vendor assessment and selection
- Assessment of completeness, accuracy and quality of business data
- Optimising technology systems through testing, validation and automated feedback
- Developing interactive reports incorporating data visualisation

pwc

[11] http://www.yonhapnews.co.kr/bulletin/2016/05/03/0200000000AKR20160503050200002.HTML?from=search

Who to contact

David Grace
Global Financial Crime Leader
T: +44 (0)20 7212 4881
E: david.w.grace@uk.pwc.com

Andrew Clark
UK & EMEA Financial Crime Leader
T: +44 (0) 20 7804 5761
E: andrew.p.clark@uk.pwc.com

Michael Weis
Luxembourg Financial Crime Leader
T: +352 49 48 48 4153
E: michael.weis@lu.pwc.com

Jeff Lavine
USA & Americas Financial Crime Leader
T: +1 (703) 918-1379
E: jeff.lavine@us.pwc.com

Vincent Loy
Singapore & AsiaPac Financial Crime Leader
T: +65 6236 7498
E: vincent.j.loy@sg.pwc.com

www.pwc.com/crimesurvey-fs

30247_MT (06/16)