WHITE PAPER

# Combating Financial Crime:

## The Increasing Importance of Financial Crimes Intelligence Units in Banking

Longitude

sas
THE POWER TO KNOW.

# Contents

# Introduction

Failing to contain financial crime hits banks with the double impact of crime-related losses and fines imposed by regulators and law enforcement agencies. Depending on the magnitude of a bank's failure to stem financial crime, fines can run into hundreds of millions of dollars – and even higher in exceptional cases. More importantly, institutions are keen to protect their brand from association with transnational organized-crime rings and scandals related to corruption.

Banks are rising to this challenge by investing heavily in staff and technologies to run their financial crimes intelligence units (FCIUs). Their FCIUs aim to mitigate reputational and regulatory risks associated with being implicated with high-profile fraud and corruption scandals such as the Panama Papers, the FIFA case and the Bernard Madoff Ponzi scheme. When a fraud or corruption scandal breaks in the media, every bank's board of directors wants to know immediately what their exposure might be. Some banks can answer this question straight away, but others are unable to.

Our research, *Combating Financial Crime: The Increasing Importance of Financial Crimes Intelligence Units in Banking*, assesses how aware banks in Europe and North America are of FCIUs and what measures they have been taking to be more prepared for full implementation of their own FCIU. We examine how FCIUs are managed and staffed, and what resourcing challenges they face as they expand. We also investigate how banks and regulators interact and whether the way they communicate with each other and with law enforcement agencies needs to change.

The research findings reveal how banks in Europe and North America are rising to the huge challenge of trying to limit the increasing levels of organized financial crime. Nearly one in five (19 percent) of the respondents in our survey of 120 banks say they have been fined by regulators or law enforcement agencies in the past three years; of these banks, 22 percent have been fined $1 billion or more.

Financial crime knows no boundaries – in fact, the exponential growth of digital communications has helped to make cybercrime one of today's fastest-growing and most sophisticated industries. Organized, transnational criminal groups operate across established crime networks to commit fraud, launder money, and finance terrorist groups and organized criminal gangs.

The FCIU is a relatively new concept that has gained traction since the global financial crisis, and financial institutions are now determining how their FCIU function can stop crime across the whole of the organization. Banks conduct ongoing organizationwide assessments of the threats, and feed the results into their central intelligence systems to help them build a full picture of the magnitude of financial crime risks. This process enables banks to formulate strategic policy decisions to combat the threat of highly organized and sophisticated financial crime.

A key reason a bank invests in personnel and technology for its FCIU is because the traditional approaches to combating financial crime are not working. Encouragingly, our research shows that 82 percent of the banks surveyed have set up an FCIU or are planning to; of these banks, a resounding 98 percent say that their FCIU is a top corporate priority.

Nearly one in five of the respondents in our survey of 120 banks say they have been fined by regulators or law enforcement agencies in the past three years.

The banking industry has earmarked billions of dollars to fund the continued rollout of cross-bank FCIUs. It is looking beyond short-term wins to implement sustainable and effective enterprisewide functions. Some 70 percent of banks in our research plan to increase their FCIU budgets over the next three years.

We discuss how technology solutions are likely to develop quickly over the short term, equipping FCIUs with sophisticated tools to combat the increasingly sophisticated threats of financial crime.

We hope that this report increases understanding of the importance of banks' FCIUs and the tremendous potential these central intelligence services will offer to the banking industry and to crime prevention.

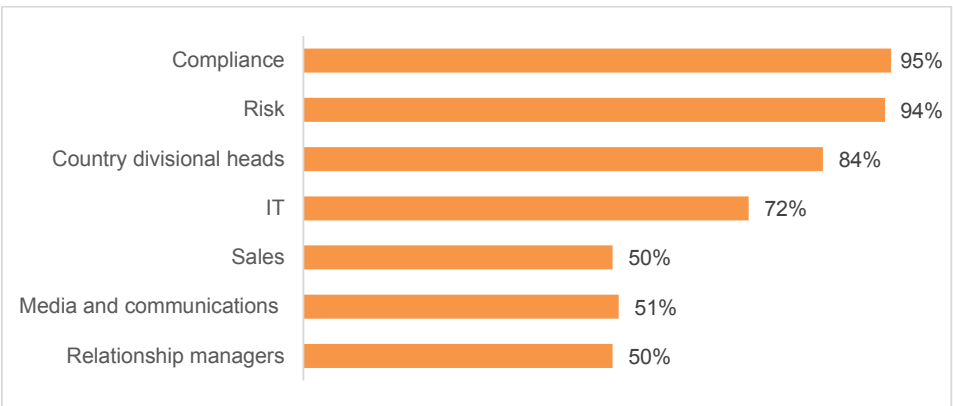
## The FCIU is embedded in banking culture

For as long as banks have traded, they have been targeted by criminals. Unsurprisingly, then, there is universal acknowledgment of the threats of financial crime. For many banks, combating these threats has become a core objective, and our research reveals that 82 percent of banks either have an established FCIU or are in the process of creating one.

"Our FCIU is part of our overall work to combat financial crime, which has been the No. 1 objective of the group over the last couple of years," says the head of a global bank's FCIU. "It's now one of two top objectives, alongside our growth aspirations."

Supporting the importance of FCIUs in the banking industry, our research shows that almost all respondents (98 percent) believe their FCIU is a top corporate priority, and 94 percent say that combating financial crime across the institution is a top training priority. Chart 1 shows that the compliance and risk functions have the highest level of awareness of the FCIU.

Chart 1. Job functions with "great awareness" of their own bank's FCIU



Many banks have established board-level committees that examine the threats and their own vulnerabilities. They make sufficient investments, aiming to prevent and deter financial crime from infiltrating their organization. Most take a reactive approach to investigation today, but they expect technology to facilitate more proactive approaches as their FCIU develops (See "Four layers of control" sidebar below).

"Our FCIU is a very high priority, and there is plenty of investment in terms of people and initiatives that go across the organization," says Matthew Rees, Senior Vice-President for Fraud and Financial Crimes at Citi in the UK. "It is given strong support both in terms of practical measures and people."

Each bank has its own approach to the way the various types of financial crime are managed. Citi, for example, has teams that focus on fraud, anti-bribery and corruption, and other financial crime, across divisions such as institutional clients and retail banking. Rees explains that these groups come together regularly to share intelligence and best practice, and to push forward joint initiatives.

Most banks have started to roll out their FCIU on a gradual basis: 35 percent say they started with a small-scale pilot project, while more than a quarter (27 percent) say they started with a specific division and 16 percent say they focused on an individual geography first. Nearly one in five banks (18 percent) have taken a whole-bank approach to launching their FCIU, which involved sunsetting existing systems.

Most banks have started to roll out their FCIU on a gradual basis: 35% say they started with a small-scale pilot project, while more than a quarter say they started with a specific division and 16% say they focused on an individual geography first.

## Geographic challenges for banks

Geographic factors are important for banks – particularly, of course, for those with banking operations in multiple jurisdictions. This not only creates more potential entry points for financial crime, but also raises complex data management and data privacy considerations.

While banks' FCIUs are generally well prepared on a multi-jurisdictional and cross-divisional basis, there are some improvements to make. Our research finds that 71 percent of banks say they are equally prepared in all of the jurisdictions they serve, and 65 percent say they are equally prepared in all sectors. The more markets in which a bank operates, the more potential challenges it faces in combating financial crime. Some international banks have to manage more than100 regulator relationships, for example.

"There is an asymmetry in understanding around FCIUs between US-centric organizations and non-US-centric organizations," says Patrick Craig, EMEIA Partner for Compliance Technology at EY. "Banks that are operating in the EMEA or Asia Pacific regions are dealing with a high number of borders, so this escalates the priority to establish an FCIU-like capability."

Standard Chartered Bank operates across many international markets – particularly across Asia Pacific and the Middle East – and has encountered specific regional issues that created the need to adopt a regional approach for its FCIU.

"We certainly continue to have a global team, but now we have individuals in our core regions who specialize in regional intelligence matters," says Nikhil Aggarwal, Head of Surveillance Parameter Optimization & Tuning and Group Financial Crime Compliance at Standard Chartered. "We operate in some high-risk geographies where we need more support, and more headcount to address the local issues."

### Data movements

Geography is a huge consideration for banks that need to manage data movements in order to share intelligence across their institutions. While some countries prohibit the export of data altogether, others have strict data privacy laws, and some have no data protection at all. This has resulted in a regionalization of some banks' FCIUs.

"Global banks often establish regional operational hubs to align with the cultural and demographic nuances of their business," says David Stewart, Director of Financial Crimes Solutions for SAS in the US. "This distributed model can present challenges for providing a holistic and consistent approach to managing risk."

## Top priorities for FCIUs

The rapid growth of increasingly sophisticated and diverse financial crimes continues unabated, creating enormous challenges for banks. They need to prioritize how to fight financial crime, and their FCIU is a key line of defense. However, an important element in this fight is their management of complex relationships with financial regulators. This has the potential to create a conflict of priorities, as the banking industry is increasingly focused on managing regulatory scrutiny rather than the root causes of crime.

FCIUs enable banks to collect or share and disseminate intelligence across borders, across business lines, and across silos of risk, where ordinarily that intelligence is not shared. "They've existed because of very specific enforcements from US regulators," says EY's Patrick Craig. "The two most notable cases were the Bernard Madoff Ponzi scheme[1] and the HSBC Mexican drug-money laundering case.[2] These examples identified gaps in banks' abilities to share intelligence across borders."

Reducing fraud is the top priority for banks. Our research shows that 70 percent of banks say their FCIUs are focused on reducing fraud loss. A geographic split exists, however: 83 percent of North American banks say fraud loss is a key focus area, compared with just 57 percent of banks in Europe. More than four in five (83 percent) of all banks with annual EBITDA growth of 10 percent or more say that reducing fraud is a key objective for their FCIU.

### Four layers of control

Depending on the resources and maturity of their FCIU, banks will adopt a variety of approaches to combating financial crime – from reactive investigations to more sophisticated, proactive detection. Most banks today take a more reactive than proactive approach.

#### Reactive investigations

As certain events occur, such as the Panama Papers and the FIFA scandal, names arise that banks will want to investigate. They will investigate whether they have any exposure to fraudulent activity, illegal money movement or terrorist activity.

#### Strategic analysis

This level of analysis is when banks want to know if they are facilitating certain activities, such as human trafficking, fraudulent money services, or money movements from sanctioned countries.

#### Proactive detection center

If an individual has multiple alerts across multiple systems, this will give a bank a fuller view of risk if it can be detected. Having a centralized function in place helps a bank to proactively detect risks it faces.

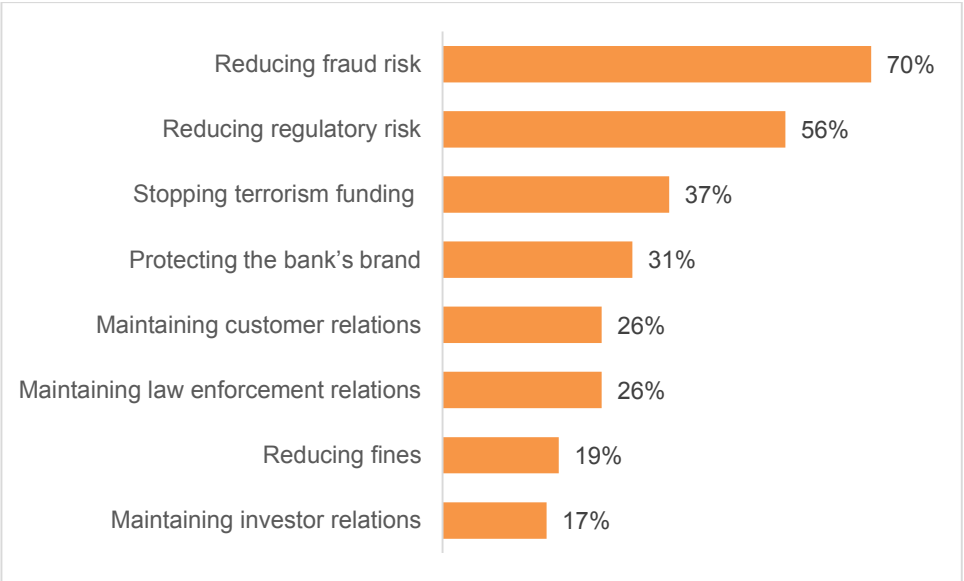
#### Optimization and coverage assessment

Optimization and coverage assessment enable banks with an existing anti-money laundering platform to assess how well that platform is detecting money laundering, what its accuracy is, and whether there are any gaps in coverage.

[1] In a response to the Madoff investment scandal, in 2014 the US Financial Crimes Enforcement Network (FinCEN) assessed a $461 million civil money penalty against JPMorgan Chase for its failure to file suspicious activity reports (SARs) against Madoff's investment firm. It was found that the bank's British intelligence unit had filed SARs on Madoff, while the US intelligence unit had failed to do so. https://www.fincen.gov/news_room/ea/files/JPMorgan_ASSESSMENT_01072014.pdf

[2] In 2012, HSBC was forced to pay a record $1.9 billion after US prosecutors said the bank willfully flouted US sanctions and was guilty of a "blatant failure" to implement anti-money laundering controls.

Chart 2. The main areas of focus for FCIUs




Increasingly, following the 2008 global financial crisis, banks have had to repair their damaged reputations and manage complex stakeholder relations, including intensified scrutiny from financial regulators. Over half (56 percent) of banks say their FCIU is focused on reducing regulatory risks, and this is split evenly across Europe and North America. More than three-quarters (78 percent) of banks with annual EBITDA growth of 10 percent or more say that reducing regulatory risk is a key priority.

## Regulatory risk management is paramount

Banks want to be able to fully prioritize mitigating financial crime risks, but according to one bank FCIU source the banking industry is increasingly focused on "appeasing" the growing pressure of regulatory scrutiny.

"One hit from a regulator can splash your institution's name across the front pages," says Citi's Matthew Rees. "Banks take a lot of time to understand what regulators' focus and direction are, what their objectives are, and their overall concerns about the whole banking industry."

Although banks are keen to avoid any damage to their brands, many regulatory actions become public despite legal attempts by banks to contain the details of a specific case. "Loss of reputation is a higher priority for many banks than limiting actual losses, but it is the most difficult loss to measure," Rees says.

A cease-and-desist order issued by the Office of the Comptroller of the Currency in the US against Citibank in 2012 for violating the Bank Secrecy Act (BSA) and its underlying regulations created huge cost implications for the bank. The order required the bank to take comprehensive corrective actions to improve its BSA compliance program, which included hiring about 2,000 staff for its compliance function.[3,4]

The research shows that 70% of banks say their FCIUs are focused on reducing fraud loss. A geographic split exists, however: 83% of North American banks say fraud loss is a key focus area, compared with just 57% of banks in Europe.

[3] Citigroup Consent Order, March 2013 https://www.federalreserve.gov/newsevents/press/enforcement/enf20130326a1.pdf

[4] Fitch Ratings (2013) More Banks Facing U.S. Anti-Money Laundering Scrutiny https://www.fitchratings.com/gws/en/fitchwire/fitchwirearticle/More-Banks-Facing?pr_id=787636

Larger banks, with more complex, multi-jurisdictional operations, are more likely to have been fined by regulators for financial crime-related activities. This reflects the complexity and vulnerability of their banking operations. Of the 19 percent of banks in our research that say they have been fined by a regulator over the past three years, two-thirds of those with revenues between $75–100 billion and over a third (36 percent) of those with revenues greater than $100 billion have been fined in relation to financial crimes.

Some industry commentators believe that increased regulatory scrutiny and actions are redefining what a bank's role should be.

"A bank has a duty to look after money and make sure that the money is safe – if I have an account with a bank, I want to know I can get my money back," says Jackie Harvey, Professor of Financial Management and Director of Business Research at Newcastle Business School. "What we're doing is creating a mechanism in the banking industry whereby banks are motivated to avoid fines and the reputation loss that goes with them. I would question whether we have pushed things too far."

Professor Michael Levi at Cardiff University says: "Some financial crimes have hit the banks or their customers, and other banks have been accused of being enablers of crimes. In a sense, these cases relate to what criminologists call third-party policing roles. Banks are not just combating crimes against themselves; a duty has been imposed on them to police crimes committed against other people."

Although banks may accept this duty, some financial crime experts say it is debatable how deeply ingrained this level of acceptance has become in the banking industry. There is an "undercurrent of reluctance" that means banks might be holding back on their monitoring activities so that regulators do not expect even more from them, says DML Associates' Dennis Lormel, a subject-matter expert in the anti-money laundering, terrorist financing and fraud communities.

"Consequently, the cost of doing more can become burdensome," he adds. "I think some institutions have chosen to take a more conservative approach and develop their capabilities in an incremental fashion."

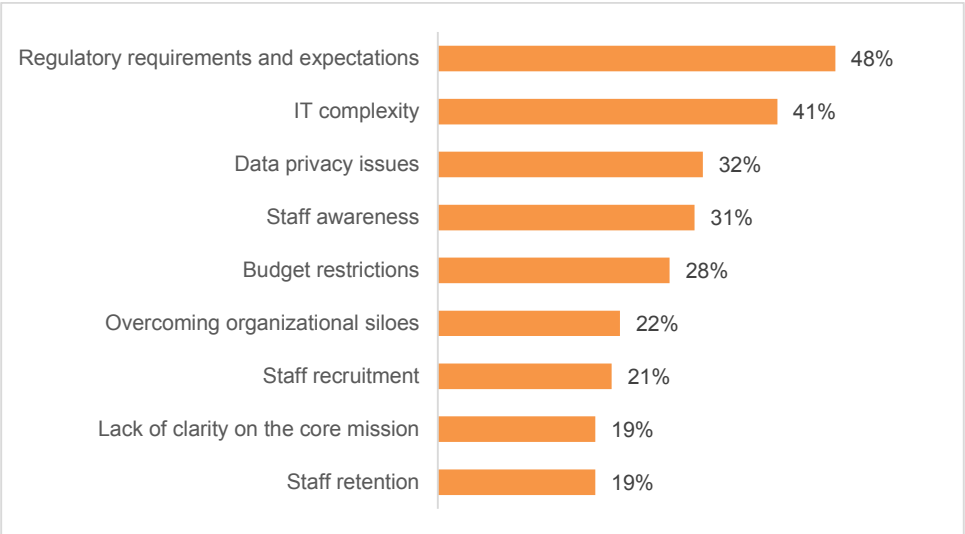
Over half of banks say their FCIU is focused on reducing regulatory risks, and this is split evenly across Europe and North America. More than three-quarters of banks with annual EBITDA growth of 10% or more say that reducing regulatory risk is a key priority.

## Hurdles hamper FCIU success rates

Banks are improving their ability to fight financial crime, but many financial institutions still face considerable hurdles. Nearly a fifth (19 percent) of banks in our research have been the subject of public regulatory enforcement action and have incurred monetary penalties during the past three years because of a financial crime that involves their institution.
So it is clear that many banks still face considerable hurdles.

Key hurdles that banks face when implementing their FCIU include regulation, IT and data challenges, operational deficiencies and staff issues (see Chart 3). FCIU implementation is still a work in progress for many banks: more than half (56 percent) of those in our research say that the implementation process for their FCIU "appears to be endless." Just 11 percent of banks say they have fully established FCIUs across all geographies and divisions of their bank. Nearly half (49 percent) of all banks say they will have a fully established FCIU in three years' time.

Chart 3. Key hurdles that banks face when implementing their FCIU




## Poor communication

While banks today face heightened scrutiny from regulators, communication between banks, regulators and law enforcement agencies needs to be improved. There are various established ways for the different agencies to come together – such as anti-human trafficking and cybersecurity forums – but there is some concern that regulators are observing more than proactively participating.

"Imagine a triangle with financial institutions, regulators and law enforcement agencies at each point," says DML Associates' Lormel. "There are solid black lines from the regulator to the financial institution and from law enforcement to the financial institution. But there is a broken line from the regulators to law enforcement."

Consequently, banks could be said to be serving two masters: the regulator and law enforcement agencies. Transaction monitoring and identification of suspicious activity exist so that the banks can provide law enforcement agencies with the information they need to either predicate or enhance an investigation.

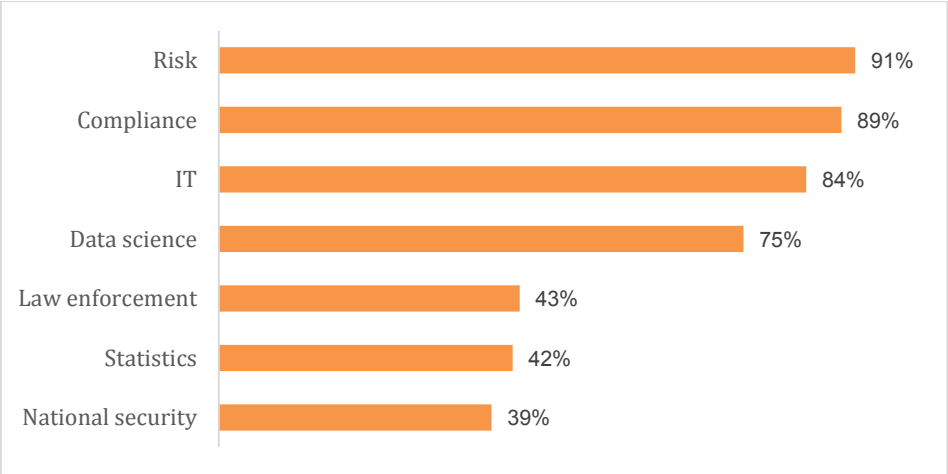
"I don't think law enforcement agencies and the regulators have traditionally taken the time to understand each other's perspectives and to work together to come up with a middle ground to get better information from financial institutions," says Lormel.

Just 11% of banks say they have fully established FCIUs across all geographies and divisions of their bank. Nearly half of all banks say they will have a fully established FCIU in three years' time.

## Talent is limited

Banks generally agree that hiring specialist talent for their FCIU is difficult: 71 percent share this sentiment. Banks with annual revenue of less than $10 billion and those with EBITDA growth of 10 percent or more express higher than average difficulty in hiring (74 percent and 94 percent, respectively).

Chart 4. Backgrounds of staff in banks' FCIUs




Risk, compliance, IT and data science dominate the backgrounds of staff in banks' FCIUs (see Chart 4). When they hire staff, banks tend to focus on specialist groups: 85 percent of banks look for staff among cybersecurity professionals; 84 percent seek staff from software companies; 61 percent from universities; and 50 percent from the government intelligence community.

The required IT skills broadly come under big data, including data science, and other sciences such as astrophysics. The ideal candidate would be someone with that sort of background, along with crime expertise and business experience. They should be able to manipulate large blocks of complicated data, says one FCIU source.

When they hire staff, banks tend to focus on specialist groups: 85% of banks look for staff among cybersecurity professionals; 84% seek staff from software companies; 61% from universities; and 50% from the government intelligence community.

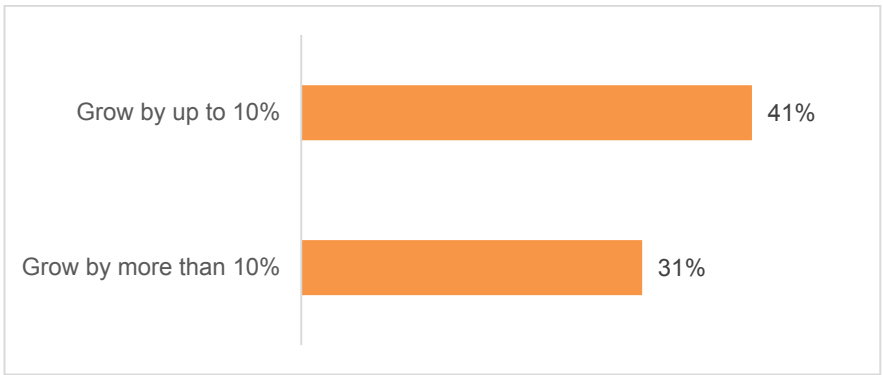
# Technologies will drive FCIU success

As banks migrate more of their businesses to digital platforms, they face increased threats, as a very large – and rapidly growing – part of the criminality that banks have to contend with is classed as cybercrime. Criminals take advantage of weaknesses in the banking system, such as banks' geographical silos and faster digital payments and processing methods.

Implementing advanced technologies and data storage platforms will underpin an FCIU's success in proactively combating financial crime. This success will be driven by teams of analysts that have the skills to manage client and thematic reviews through very effective, and legal, data analysis. Although banks are taking considerable measures to invest in IT solutions, this field is growing rapidly, which means banks will need to ensure that their budgets keep pace.

When it comes to state-of-the-art IT, our research shows that 78 percent of banks agree that they have this in place today. Almost four in five banks (79 percent) say they have an IT budget that will help them to combat financial crime. Banks are investing in the FCIUs and many are planning to increase their budgets considerably, as Chart 5 shows.

Chart 5. FCIU budget growth over the next three years




However, banks face huge challenges in trying to bring together as much useful data as they can within the legal constraints of the different jurisdictions where they operate. "Our objective is to use data across all the places where we can legally access the data," says the head of an FCIU at a global bank. "We will be, by definition, the biggest data repository our bank has ever produced."

Banks operating across multiple jurisdictions sometimes face significant challenges around data privacy laws in different countries, which can create obstacles to their joined-up fight against financial crime. "The legal restrictions are paramount, and we have to respect the law," says the bank source. "But at each stage of our work we're trying to bring together the maximum amount of data we can."

Having a huge repository of data will be ineffective if banks are unable to get useable intelligence out of it, which means they need to be able to run sophisticated analytics.

"Almost everyone is piloting Hadoop as the underlying data storage platform, because of the variety of data sources required to analyze financial crime," says SAS' Stewart. "It's critical to connect disparate data systems and land them into one sandbox." Hadoop is a highly scalable and resilient open-source software framework with good processing power. Big data analytics stands out as the leading technology tool for FCIUs; 87 percent of banks in our research agree.

Advanced search and discovery (80 percent) and machine learning and unstructured data mining (both 70 percent) are also very popular with our respondents in our survey. Technology solutions figure highly for banks that have EBITDA growth of 10 percent or more – 100 percent of these chose big-data analysis, 94 percent chose advanced search and discovery, and 67 percent chose machine learning.

Technology solutions figure highly for banks that have EBITDA growth of 10% or more – 100% of these chose big data analysis, 94% chose advanced search and discovery, and 67% chose machine learning.

"There are exciting opportunities in terms of assimilating data from different sources very quickly, structuring the data, and obviously deploying analytics. By that, I mean, for example, text mining," says Standard Chartered's Aggarwal. "If you look at a narrative on a particular client, what are some of the key words that are emerging? This can include link analysis, funds moving from different sources and different counterparty activity."

A key focus for FCIU units will be to have teams that understand criminal behavior and those that can focus on specific transactions. Banks will need to integrate and structure the data, and be able to look through both lenses. Analytics has a key role to play. First by structuring and integrating the data and finding more simple outcomes like correlation and causality, and then by moving into more predictive models.

Analytics can mean different things to different people, however. Financial institutions need to use clear definitions. A data request could collate transactions over a certain time frame, while a business intelligence request could flag up a given trend over a certain period. Neither, however, are analytics.

"We're just getting started in terms of true machine learning," says Aggrawal. "In three years' time I would expect an analytics team to point out anomalies in the data. That's kind of the shift I'm expecting in terms of proactive analysis."

## Key takeaways

1. Banks have very strong awareness of financial crime, but the threats are continually evolving and multiplying. Banks need to concentrate on rolling out their FCIUs across the whole organization in a phased and focused way in order to be as effective as possible.

2. To achieve their FCIU expansion plans, banks need to maintain a realistic focus on their budget and resourcing requirements.

3. To help create a new generation of financial crime experts, banks need to ensure that they encourage a flow of diverse, talented recruits into their FCIUs.

4. Banks should make full use of the information they have about cyber risk, failed authentication attempts, abnormal session behavior and geolocation data. Every detail can provide vital clues in the financial crimes investigations.

5. Banks should weigh the benefits and costs of building best-of-breed systems relying heavily on open-source technologies versus best-of-platform capabilities offered by commercial software vendors. Big data technologies are evolving rapidly, and the search, entity-resolution, text-mining and link-analysis processes adopted by FCIUs present changes to business process. Change management and integration are key to a successful rollout.

6. A unified front line against sophisticated financial crime gangs is needed as a priority. To make this a reality, banks, regulators and law enforcement agencies should communicate more effectively and collaborate more efficiently.

# About the research

Longitude Research surveyed 121 investment and commercial banks in early 2016, equally split across Europe and North America

Respondents represented a range of functions within banks, comprising risk (29 percent), compliance (28 percent), finance (20 percent), anti-money laundering (8 percent), financial crime prevention (8 percent), and fraud prevention (8 percent).

Longitude asked each respondent a series of detailed questions about their financial crimes intelligence unit, focusing on their bank's awareness and preparedness; corporate strategy; and implementation considerations and hurdles.

The key findings from the quantitative research were combined with output from a series of qualitative interviews with industry experts to produce this insightful report.

A special thanks to the following experts for taking part in in-depth interviews for the research:

- Nikhil Aggarwal, Head of Surveillance Parameter Optimization and Tuning, Group Financial Crime Compliance, Standard Chartered Bank
- Patrick Craig, EMEIA Partner, Compliance Technology, EY
- Jackie Harvey, Professor of Financial Management and Director of Business Research, Newcastle Business School
- Michael Levi, Professor of Criminology, Cardiff University
- Dennis Lormel, DML Associates
- David Stewart, Director of Financial Crimes Solutions, SAS
- Matthew Rees, Senior Vice-President for Fraud and Financial Crimes, Citi

To contact your local SAS office, please visit: sas.com/offices