McKinsey & Company

Risk Practice

The investigator-centered approach to financial crime: Doing what matters

The investigator-centered approach to fighting financial crime fosters collaboration among banks, law-enforcement agencies, and regulators for greater effectiveness, efficiency, and social impact.

By Adrian Murphy, Kate Robu, and Matthew Steinert

May 2020

Over the past ten years, the level of activity in financial-crimes compliance in financial services has expanded significantly, with regulators around the globe taking scores of enforcement actions and levying $36 billion in fines. Many financial institutions have scrambled to implement remediation efforts. Financial-crimes compliance (FCC) was elevated as a function, often reporting to the chief risk or compliance officer. Staffing levels and the organizational seniority of the first and second lines of defense were greatly amplified. The activity generated has cost large institutions hundreds of millions annually and created a dynamic marketplace for consulting services and technological solutions.[1]

Technology in fact now accounts for a significant part of the financial-crimes budget. The demand has generated myriad offerings by incumbent and new vendors, which vie for the chance to alleviate their clients' many pain points. Regulatory-technology start-ups have attracted billions of dollars in investment in recent years, the bulk of it focused on know-your-customer and anti–money laundering (KYC/AML) use cases. Despite this trend, most banks report that manual processes persist. When asked, banks say that as much as 85 percent of FCC and AML activities remain administrative or nonanalytical in character (such as the manual collection of data from some systems to import into others).

The current approach, as expensive as it is, is focused on regulatory compliance. Not surprisingly, it has not been very effective in identifying and intercepting financial crime. Estimates of the volumes of funds moved through the global institutional system in proscribed transactions range from $800 billion to $2 trillion annually. The same estimates indicate, however, that the authorities intercept less than 1 percent of those amounts. The leak of the so-called Panama Papers, the files of a large offshore law firm, is a case in point. The papers showed rich and powerful individuals exploiting offshore tax regimes by funneling their wealth through hundreds of thousands of offshore companies. Not all the activity uncovered in the leak was illegal, but much of it was—*and none of it had been recognized in routine KYC/AML activity.*

To experts, this is not surprising, actually. When asked, most financial-crime AML practitioners will say that their focus is on ticking boxes for regulatory compliance rather than investigating leads and intercepting proscribed movements of funds.

Further evidence of the institutional focus on procedural compliance is the high number of defensive suspicious-activity reports (SARs). Filings have proliferated partly because the tools used for transaction monitoring and due-diligence processes are astoundingly inaccurate. Only one or two transaction-monitoring alerts per hundred is typically acted upon, for example.[2] Another example, from the world of due diligence, is illustrated in Exhibit 1. It presents a typical multifactor customer risk-rating model for the retail business of a large North American universal bank. A manually conducted expert review of the results revealed that for every 100 customers rated high risk, 72 were actually medium to low risk; furthermore, 57 of every 100 customers rated medium to low risk by the model proved on review to have a high-risk profile. To put this into perspective, a credit-risk model with this kind of performance would never be allowed into production.

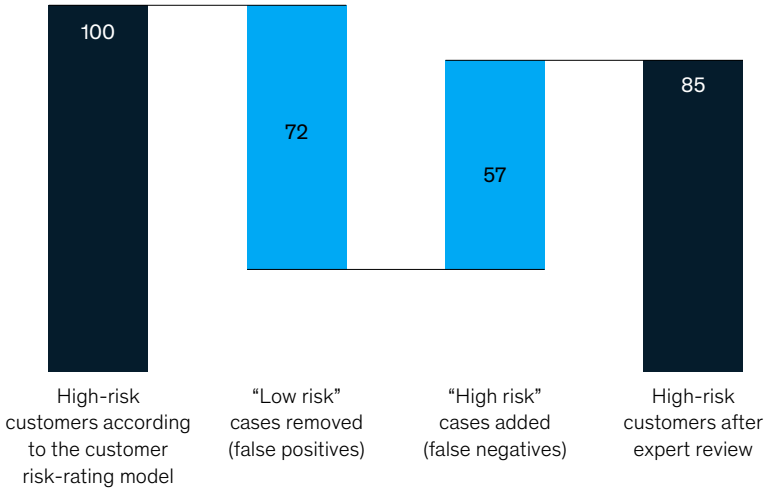
Unfortunately, most of the effort and resources invested in the industry today are focused on optimizing the status quo. These adjustments, such as calibrating thresholds for transaction-monitoring alert scenarios, adding more factors to the existing customer risk-rating models, and automating data feeds throughout the current process, have yielded only incremental improvement. If we were discussing aircraft design, an exorbitantly expensive problem-solving approach that addresses at most

[1] McKinsey Compliance Benchmarking 360 Survey, 2019.
[2] For most banks, more than 90 percent of transaction-monitoring alerts turn out to be false positives. Of those alerts that do result in a suspicious-activity-report filing, 80 to 90 percent are not acted upon.

Exhibit 1

The customer risk-rating models banks employ to detect proscribed transactions under KYC/AML mainly produce false positives and false negatives.

High-risk customers sent to enhanced due-diligence units (disguised real data example), indexed to 100



2 percent of the problem would have been set aside long ago. An increasing number of FCC/AML practitioners believe that the industry needs to go back to the basic premise of combating financial crimes. They want to clarify the mission and define a set of realizable objectives. They want a solution, in other words, that will actually *fly*.

As many industry leaders have pointed out, regulatory reform in FCC/AML is needed to help the industry shift its focus—from reducing the amount of unidentified potentially suspicious activity to increasing the amount of identified actual criminal activity.

While awaiting regulatory reform, institutions can significantly improve efficiency and effectiveness in other ways. They can work with regulators and their own internal audit group to eliminate low-value activities, automate more processes, and implement more advanced analytics. They should also develop investigative capabilities.

Some have already begun to shift their thinking in this direction. Since an investigative approach produces more meaningful results for law enforcement, it also accelerates the momentum for change. Realignment from procedural compliance to an investigator-centered approach will take time, so early movers will have a number of advantages. They will be better positioned to influence regulatory reform by redefining the meaning of effective FCC/AML. Early movers will also save more, as they divert investment away from ineffective solutions toward the technology and data needed to support the new capabilities. As these capabilities demonstrate positive impact in customer experience and overall effectiveness, institutions can begin to reduce structural costs by removing ineffectual activities.

Since the investigator-centered approach is aligned with the spirit of existing regulatory guidelines, financial institutions do not have to wait for formalized regulatory change. If they can prove that their FCC/AML activities are more productive, they

can begin to eliminate the unproductive activities even under the current regime.

From filling out forms to following real leads

The new approach proceeds from a single tenet: follow the investigator. The overwhelming majority of productive alerts—those that lead to enforcement investigations—originate with inquiries from law enforcement or other relevant external partners and "negative news"—publicly available risk-relevant information. Some productive leads also come from targeted analyses of outliers and anomalies. Most important for our discussion, however, is that relatively few investigative cases are *triggered* by automated alerts and the SAR-generating activities associated with them.

In the new approach, banks pursue high-quality leads, including specific requests from law enforcement, names or addresses associated with known transgressions, or known high-risk locations or websites. By focusing organizational FCC/AML resources in this way, banks will dramatically reduce false positives. In the United States, for example, 95 percent of investigations submitted in response to information-sharing requests by the Financial Crimes Enforcement Center (FinCEN) yield positive results. A leading institution that set up an intelligence-based investigations unit reports productive outputs in excess of 80 percent. Without such information sharing or tangible leads of some kind, less than 2 percent of alerts achieve productive results.

One argument in favor of the current SAR filing process is that it is the primary means financial institutions use to pass on information to law enforcement. FinCEN reported that law-enforcement agencies consult the SAR database 30,000 times per day, estimating a total of 7.4 million queries in 2019.[3] Our research suggests, however, that the searches are often performed to support existing cases or follow leads. Given that pattern of usage, the database could become a more comprehensive and efficient tool were banks to provide it as primary data on an automated basis. Accordingly, law enforcement would be given more access to searchable bank data, as long as all applicable privacy laws and protections were respected (such as safe-harbor provisions). At the very least the process and tools for information exchange between financial institutions and law-enforcement agencies could be significantly improved, thus eliminating the need for massive (and often unnecessary) SAR writing and filing.

Another issue with SARs is that most of the information banks recover from them amounts to fragmentary evidence of past activities. While they are useful for building prosecution cases, the delayed and incomplete bits are of less use to banks for the prevention of financial crimes than a more up-to-date and holistic view would be.

In contrast, the new approach puts investigative teams at the center of efforts against financial crime. Teams begin with seemingly small pieces of high-quality information, developing leads through intelligent follow-ups and probing. The objective is to intercept proscribed transactions and bad actors quickly. Investigators are encouraged to be proactive, connecting financial transactions and other information (such as travel or shipping itineraries, tax filings, trade invoices, and predicate crimes), using advanced analytics and new data sources. Over time, by connecting the dots in this way, institutions build a better understanding of customer behavior and the sources of risk.

Banks could object to an approach requiring them to develop investigative capabilities, countering with a traditional view that investigating financial crime is law enforcement's job. The role of banks, in this view, is limited to identifying and reporting

[3] "Prepared remarks of FinCEN Director Kenneth A. Blanco," delivered at the American Bankers Association /American Bar Association Financial Crimes Enforcement Conference, December 2019, Financial Crimes Enforcement Network, December 10, 2019, fincen.gov.

The best way for financial institutions to allocate FCC/AML resources is to set investigators to work on cases based on some kernel or snippet of information that points to unlawful activity.

unusual, suspicious, or potentially unlawful activity. Increased investigative efforts by banks would not only add to FCC/AML costs but also heighten regulatory expectations for the level of assistance banks provide to law enforcement. There is logic in this view, but the reality is that it has led to a status quo few financial institutions would deem efficient or effective. The new approach promises both improved FCC/AML results and lower costs.

A good working relationship between financial institutions and law enforcement, particularly at local-office level, makes this lead-based, clue-driven investigative approach possible. It helps banks gain visibility into emerging risks and bolsters public trust. The approach does, however, signify a shift in mindset compared with the current regulatory-driven approach. How should institutions proceed? We see five constituent actions.

1. Focus on sources of productive leads

This is the heart of the investigator-centered approach. The best way for financial institutions to allocate FCC/AML resources is to set investigators to work on cases based on some kernel or snippet of information that points to unlawful activity. As previously mentioned, the leads come from inquiries from law-enforcement or other external partners, negative news, and, to a lesser extent, analysis of abnormal activity. Collaboration with external partners, including law enforcement, is discussed in action four, below. Analysis of abnormal activity (also known as anomaly detection and outlier analysis) can become a much-improved source of productive leads with the use of modern analytical techniques. (It is a topic to which we will dedicate a technically focused article in the near future.)

Negative-news screening (also known as adverse-media screening) has been recommended by regulatory authorities in high-risk situations for some time, as part of enhanced due-diligence procedures. These do not often require continuous monitoring of negative news, but examiners have lately been expressing concern over the effectiveness of the monitoring process. This suggests that the bar may be rising, and institutions might eventually be required to apply negative-news screening in more situations and to more categories of customers.

Many financial institutions still use manual approaches for negative-news screening. With many third-party solutions available, however, they can automate this process. Investments in artificial intelligence (AI) and digital tools can dramatically improve the reach of the screening and the quality of insights it will surface. Available solutions produce potential leads but also sets of insights to help analysts assess and prioritize information in the broader context of the case. When selecting among vendors of these solutions, banks will want to consider the negative-news sources they offer;

their coverage by country, language, and customer; and the array of technical features listed, including the following features:

— data acquisition by keyword search to retrieve articles

— natural-language processing to analyze language usage and extract a set of features (such as related people and mixed-case names)

— association model to relate searched entities and articles (from unassociated to highly associated)

— event-classification model to organize by article topic (known as "event type")

— grouping of articles by subject or incident within each event type

— auto-adjudication to highlight potential false positives

— workflow functionality, including audit traceability, visualization, and integration with other tools

2. Assemble agile cross-functional investigative teams

The financial-crime investigator of the future will not be an individual but a cross-functional team. It will include former law-enforcement agents; business, fraud, and cyber experts; product specialists; data scientists; and financial analysts. The team will thus be well positioned to connect the dots in a case. In rapid development cycles, the team takes in leads, substantiates cases, probes for real material risk, and stops where evidence is limited or material risk is low. The work is centrally coordinated and strictly prioritized based on the probability of a successful outcome for law enforcement. Institutions will solicit feedback from law-enforcement agencies to ensure that their lead generation, priorities, and processes are continuously improved. Exhibit 2 illustrates how agile investigative teams operate.

Some financial institutions have already created special investigative units to work on leads from law enforcement, negative news, and high-probability internal alerts. They report success rates of 80 percent and more, taking cases with high risk exposure and the likelihood of a successful outcome. The success of these units presents a stark contrast with existing industry approaches, which mainly produce false negatives and false positives. The challenge is to make this approach scalable. That requires banks to develop a scalable operating model and invest in the necessary investigative tools and data.

3. Enhance investigative tools

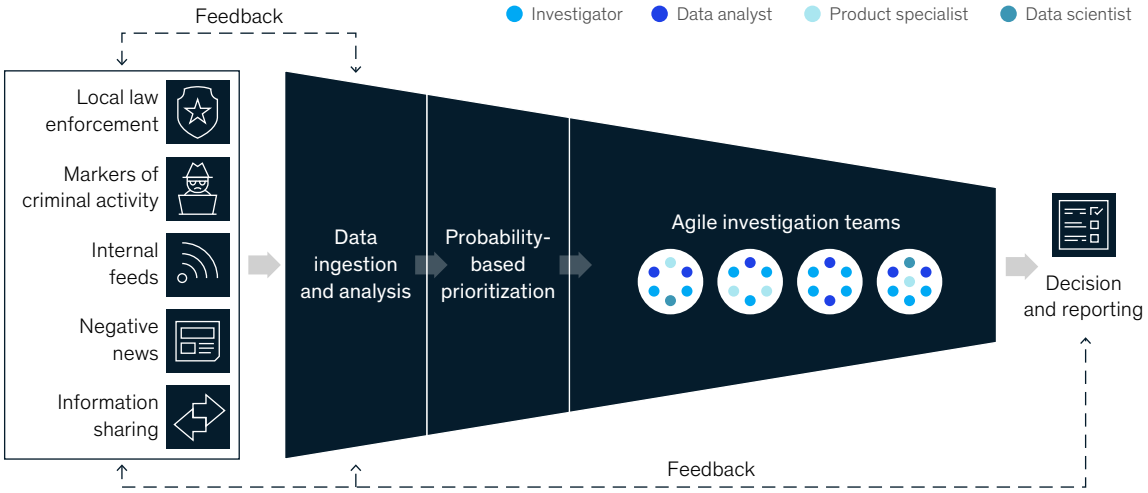
To put the investigative team at the center of financial-crimes risk management, banks must enable team members to spend the vast majority of their time investigating. Most investment in FCC/AML technology has been in internal data, models, and scenarios. Investigators have been offered little technical help, beyond workflow tools that mostly serve as task trackers and systems of record. These are rarely integrated with data sources relevant for the investigation and produce few useful insights. Investigators spend much of their time shuffling among different applications and performing a fair amount of manual data entry to create formal paper trails around cases (even for false positives).

The solution lies in deploying the data, analytics, and technology needed to free human investigators to produce better results in the highest-risk cases. The technology-aided investigation can improve outcomes dramatically, providing investigators with a more complete view of the parties and transactions involved, drawn from more diverse data sources. We will publish a dedicated article on these tools and how they work in the coming months. Here are some of the more promising enhancements:

— improved design and data visualization to inform investigators of the reason for an alert and potential courses of action (Exhibit 3 presents an example of an investigator dashboard)

Exhibit 2

The agile, cross-functional investigative team is focused on following qualified leads to identify proscribed activity.



- improved entity and network resolution to provide more clarity on high-risk connections and beneficial ownership, by using more automated data and intelligence sharing from public and private sources
- intelligent search function tailored to FCC/AML needs to produce more relevant, prioritized results
- "point and click" metrics and analysis to help investigators assess cases and determine actions
- automated prepopulation of key data items and AI-enabled text generation to support investigators in report production
- automated quality control of the output, subject to human review
- improved information storage and retrieval

4. Build a network of external partnerships

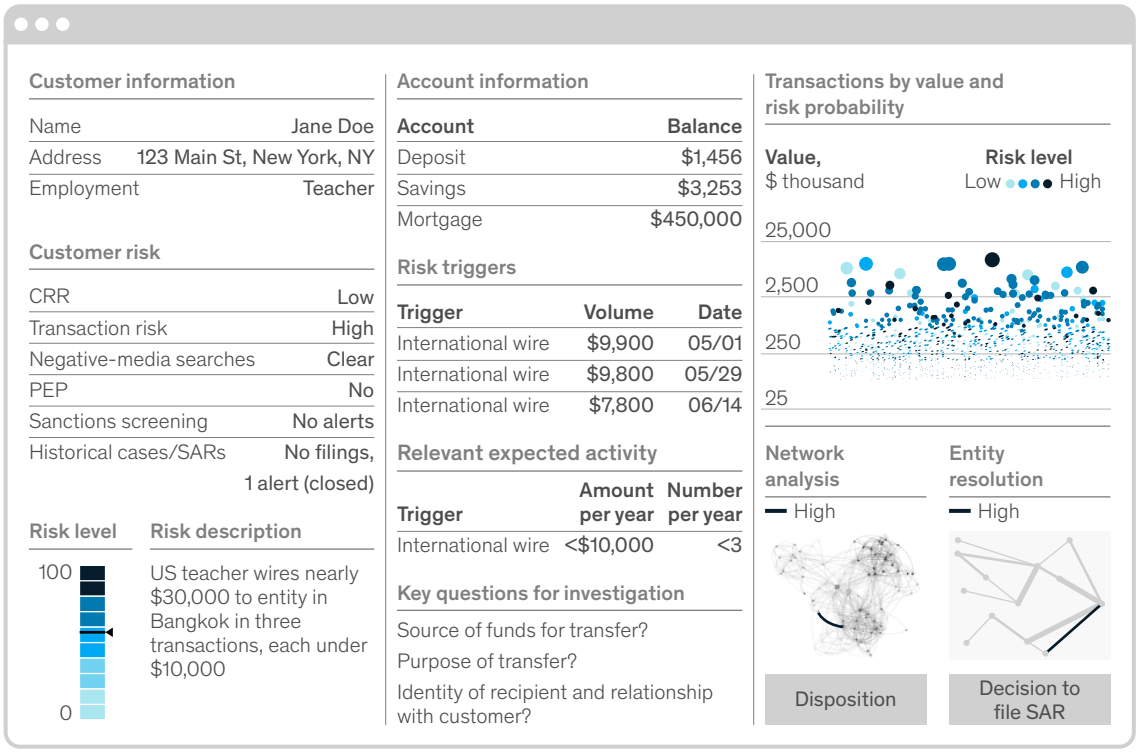
Shared intelligence is critically important for successful investigations. Collaborators include local law enforcement (for criminal trafficking), other financial institutions, tax-collection agencies, shipping companies, airlines, social-media companies, and nonprofits. In the United States, more than 100 interagency joint money-laundering task forces already exist at the federal level, and even more than that at the state level.

Collaborative networks of institutions and shared information enable more rigorous investigations. Some financial institutions have shared information with Polaris, for example, an organization that fights human trafficking. Leads and investigative insights may come in the form of potential sanctions violations, information on planned shipping routes, and retail and payments data on any number of dubious activities. With the right platform, the data

Exhibit 3

Improved dashboard design and data visualization inform investigators of the reason for an alert and potential courses of action.

Example dashboard, illustrative



Note: CRR = credit-risk rating; PEP = politically exposed person; SARs = suspicious-activity reports.

can be processed and filtered through advanced machine-learning algorithms to help investigators understand institutional exposures to the parties directly involved in the proscribed actions as well as to related parties. Investigative teams will make the connections among the flagged transactions, across all banking products and services.

Close collaboration with law enforcement is paramount, particularly at the local-office level. To build an effective operating model for this joint work, banks should bring former law-enforcement officers and specialists onto their investigative teams. Their expertise and their relationships help the institution investigate leads and better understand arising threats and local priorities. Relationships with active officers will also be instrumental in helping institutions understand the local authorities, including their processes and their people.

Financial institutions and enforcement agencies can also create public–private partnerships to improve the information flow and intercept prohibited activities. An example of such a partnership is the Joint Money-Laundering Intelligence Taskforce (JMLIT) in the United Kingdom (involving more than 40 financial institutions), the Financial Conduct Authority (FCA), Cifas (the nonprofit fraud-prevention

organization), and five law-enforcement agencies. JMLIT utilizes information from the real economy—logistics companies, airlines, retailers, hotels, and so forth. The sharing of information among industries located at different points along the chain of proscribed activities reveals a more complete picture of the nature and patterns of these activities.

5. Realign activities and platforms

While the path forward is exciting, financial institutions remain burdened by their current FCC/AML infrastructures. This limits their ability to make needed investments and allocate talent and management resources toward a more progressive solution. More important, the sheer volume of current activity and controls is deeply distracting, reducing the organization's ability to act on real risks. The "signal-to-noise ratio in the AML space," as a chief risk officer at a North American bank remarked, "is unbelievably low."

In the current absence of structural regulatory reform in this space, financial institutions should begin streamlining current FCC/AML operations to make them much more efficient and effective, while freeing up substantial resources for redirection to more valuable activities. At many institutions, FCC/AML operations were developed in reaction to intense regulatory scrutiny. Much was done quickly and under great pressure. Many banks relied heavily on industry-standard and manual solutions to save time and effort. These conditions led, unsurprisingly, to inefficient and ineffective operations, unsustainable in size and cost.

There are a few practical things financial institutions can do to substantially realign the current AML infrastructure and increase the signal-to-noise ratio.

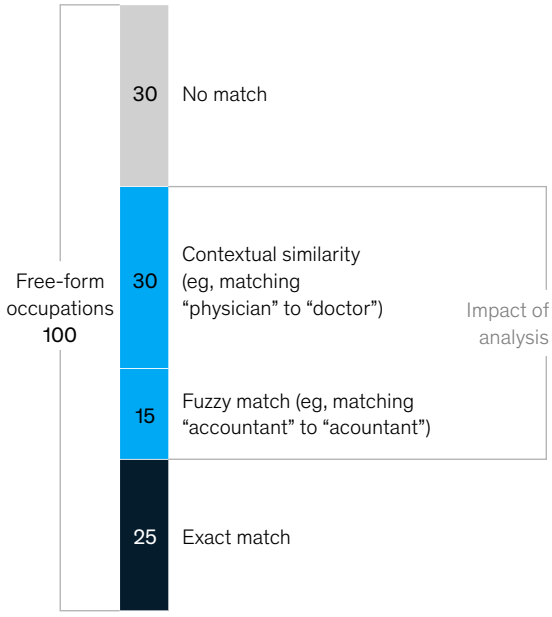
First, banks can review all FCC/AML activities and stop doing anything that is not required by regulations or beneficial to law enforcement. In our experience, institutions introduce many activities as tactical repairs but keep doing them even after they're no longer needed. Over time, layers of redundant controls and processes pile up. These should be cleared away, but with care so that the overall soundness of financial-crimes risk management is not compromised. Before removing activities that are not contributing to the effectiveness of the program, banks should of course discuss their intentions with the regulators.

Second, banks should add more intelligence to decision making, across organizational silos, databases, and systems. As an example, one North American bank used a combination of tools, including fuzzy logic and Google Dictionary, to take out 45 percent of the cases in its enhanced due-diligence pipeline. It came down to a matter of fixing data-quality issues with the occupation-code data field (Exhibit 4).

Exhibit 4

One bank significantly reduced 'noise' in its due-diligence pipeline by improving data quality.

Use of text analytics to eliminate backlogs in due diligence (disguised real data example), indexed to 100



By automating manual tasks, particularly in information and documentation management, banks can significantly reduce the strain on resources (see sidebar, "Streamlining existing FCC/AML operations: Example actions").

Particular initiatives will improve the effectiveness and efficiency of FCC/AML activities, by freeing up resources for redeployment to the actions that are truly consequential in fighting financial misdeeds. The aggregate effect of sets of initiatives can be significant. At large banks, the effects of streamlining in this way can add up to hundreds of millions of dollars (Exhibit 5).

Benefits

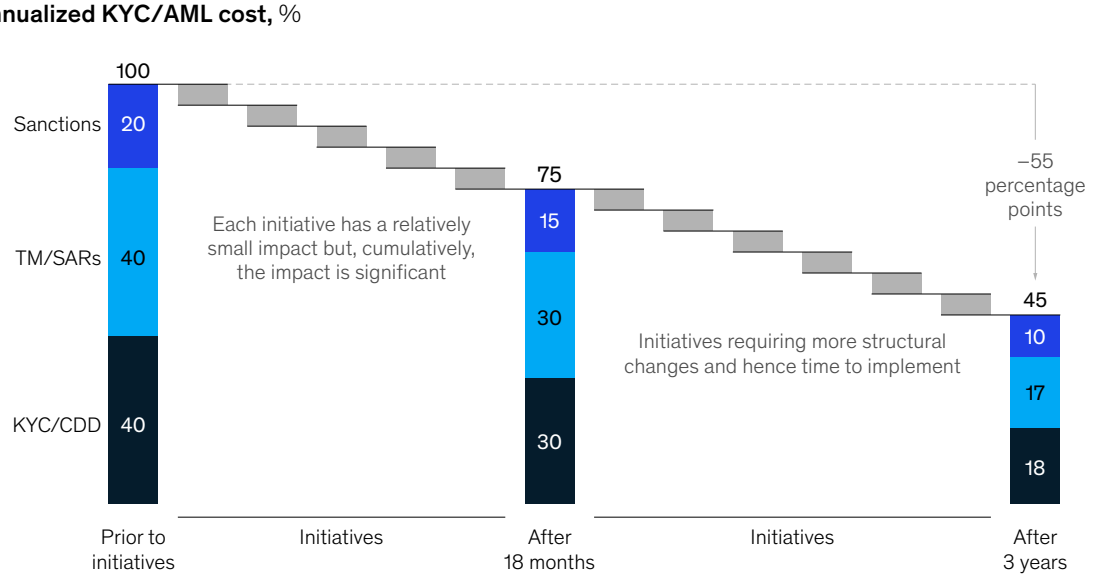
The benefits of the investigator-led approach to FCC/AML consist first of all in dramatically improved effectiveness. Activities today typically result in false-positive rates of 90 percent or more. The great majority of the work is not really useful in identifying and mitigating financial crime and proscribed transactions. The investigator-led approach is designed to reverse these proportions. It will increase the signal-to-noise ratio of current due-diligence and monitoring processes, helping to refocus efforts on the most valuable actions. Banks will be able to process far more proscribed activities.

A second benefit will be in reduced strain on organizational resources. The gains achieved from the substantial improvement of current processes and tools could be reinvested in special investigative teams that serve as much better partners to law-enforcement agencies in the investigation of crimes.

A third benefit is that the approach can elevate the profile of financial institutions as socially responsible actors in society and build public confidence in banks and the financial system. By improving detection and reducing financial crime, banks will be helping to reduce instances of money laundering, drug smuggling, human trafficking,

Exhibit 5

Financial institutions can unlock organizational resources in financial crime–related activities with a series of incrementally effective initiatives.



Note: TM = transaction monitoring; SARs = suspicious activity reports; KYC = know your customer; CDD = customer due diligence; AML = anti-money laundering.

Streamlining existing FCC/AML operations: Example actions

Eliminate unnecessary activities. Introduce event-based review cycles for low-risk customers, ensure that the due diligence performed is commensurate with risk and regulatory requirements, remove redundant checks and excess quality assurance and control (QA/QC), reduce defensive suspicious-activity reports (SARs).

Introduce more intelligence into decision making. Improve links and optimize processes across silos to elevate performance; use behavioral information to improve client risk-rating models; maximize use of know-your-customer (KYC) information to tailor transaction monitoring; dramatically reduce false positives with machine learning–based detection models; use machine learning to improve sanctions-screening and filtering algorithms to reduce "noise" and false negatives; and use smarter search algorithms, improved entity resolution, and better data visualization and management to improve investigation productivity and outcomes.

Streamline and automate processes. Automate data collection and document handling for KYC and customer-due-diligence (CDD) procedures; automate data collection and case-file assembly sourcing from internal and external sources; improve differentiation in investigative processes by improving skills and better aligning these processes with risk objectives and business value; introduce automated data-quality checks and quality assurance and control (QC/QA).

corruption, and embezzlement. Customers and society as a whole will see the results of these investigations as highly worthwhile. Research has shown that companies with improved environmental, social, and corporate-governance profiles enjoy higher shareholder value, higher equity returns, and a reduction in downside risk.

Finally, the new approach will foster deeper regulatory engagement—and that's a good thing. To improve detection, banks will need to share more information and create public–private partnerships. They cannot do all this on their own. Regulatory incentives are needed both to encourage banks along this path and to provide them with a safe harbor for testing innovative solutions as new types of previously unnoticed proscribed transactions are discovered. Some regulators have indicated their openness to innovative approaches, and financial institutions should take up this invitation. They must ensure not only bilateral senior-level involvement but also cooperation on the ground—where the innovations meet the road, so to speak.

Institutions devote a massive amount of resources to financial-crime compliance and anti–money laundering, mostly on procedure-driven activities, the effectiveness of which is rather limited. We believe the clock has run out on refining the existing model. The field is open for an intelligence-driven, investigator-centered approach that focuses on intercepting the proscribed activities of highest risk to the organization.

Adrian Murphy is a partner in McKinsey's New York office, **Kate Robu** is a partner in the Chicago office, and **Matthew Steinert** is an associate partner in the Toronto office.