McKinsey & Company

Risk

# Transforming approaches to AML and financial crime


September 2019

# Contents

# Transforming approaches to AML and financial crime

Welcome. This compendium of articles on financial crime and fraud addresses some of the most compelling risks financial institutions are facing today. The types of crimes and cyberattacks are converging, as attackers adapt to the digitization and automation of financial services. The transgressions are becoming more sophisticated, cutting across (and effectively circumventing) siloed responses. Many banks are focusing on reducing liabilities and efficiency costs, but losses in customer experience, revenue, reputation, and even regulatory compliance are mounting.

The stakes in this fight have never been higher for financial institutions. Money launderers are using increasingly sophisticated methods to avoid detection and regulators are pressing for improved efficacy in anti–money laundering (AML) programs. Globally, the laundered cash flow has been measured, in some estimates, in the trillions of dollars annually. Penalties imposed for perceived laxity in fighting financial crime have run to tens of billions of dollars and individual institutions are investing millions in AML and know-your-customer (KYC) efforts.

For these reasons, our articles are mainly focused on the strategic and technical solutions that address the variegated threat landscape. Particular attention is given to the increasingly important role of data and analytics in reducing the risk of fraud and financial crime and in helping banks meet regulatory requirements. Fortunately, regulators worldwide are encouraging the industry to adopt innovative approaches: in the United States, for example, five regulatory authorities issued a statement urging banks to keep investing in artificial intelligence and other technological advances to improve their programs.

Such powerful tools can vastly improve the effectiveness and efficiency of AML and KYC programs. Network analytics is one such tool. This can significantly improve the effectiveness of detection methods, by finding the hidden links between entities, illuminating the relationships and interconnected transactions that characterize money-laundering activity. Transgressions can thereby be detected that would have been missed by traditional models.

In KYC and due diligence, banking leaders are retiring burdensome manual approaches by applying the same digital technologies that they used to transform their commercial and operational performance. They are segmenting customers more finely to manage risk and value optimally, at minimal execution cost per customer. Digital KYC has enabled firms to remediate millions of their retail customer base, an achievement that would have been impossible with the traditional manual approach.

Another area where a step-change in efficiency and effectiveness is needed is the customer risk-rating model (CRR). One of the primary tools used to detect money laundering, CRR today is notoriously inaccurate, producing scores that miss high-risk customers and misclassify legions of low-risk customers as high risk. Institutions consequently must review vast numbers of cases manually; this drives up costs, annoys low-risk customers, and diverts AML resources that might otherwise be focused on actual money-laundering activity. By improving their data and applying better analytics, financial institutions have been able to build far more effective customer-risk rating models.

To avoid diffuse efforts and overly complex transformation programs, institutions should in our view focus first on actually mitigating risks. If programs are designed for risk effectiveness—which demands the application of advanced technologies—other benefits will be in reach. Effective AML programs limit the risk of negative regulatory findings; as regulators issue new guidance, institutions can focus on using it to improve effectiveness further, rather than taking a box-checking stance. Likewise, deploying the state-of-the-art digital solutions needed to improve AML effectiveness will also improve efficiency, where traditional

approaches add more costly checks and controls. Finally, improved effectiveness and efficiency in AML can provide a solid foundation for a better customer experience, as customer onboarding and the investigation of suspicious activity becomes less onerous.

We hope that you find these articles present compelling solutions for today's increasingly treacherous risk environment. They are the product of the efforts and experience of real companies, as they have found their way to more effective, less costly approaches to fighting financial crime.

**Kevin Buehler**

Senior Partner
Risk Practice

September 2019.

# Flushing out the money launderers with better customer risk-rating models

## Advanced risk-rating models dramatically improve detection by applying machine learning and statistical analysis to better-quality data and dynamic customer profiles.

Daniel Mikkelsen, Azra Pravdic, and Bryan Richardson

Money laundering is a serious problem for the global economy, with the sums involved variously estimated at between 2 and 5 percent of global GDP.[1] Financial institutions are required by regulators to help combat money laundering and have invested billions of dollars to comply. Nevertheless, the penalties these institutions incur for compliance failure continue to rise: in 2017, fines were widely reported as having totaled $321 billion since 2008 and $42 billion in 2016 alone.[2] This suggests that regulators are determined to crack down but also that criminals are becoming increasingly sophisticated.

Customer risk-rating models are one of three primary tools used by financial institutions to detect money laundering. The models deployed by most institutions today are based on an assessment of risk factors such as the customer's occupation, salary, and the banking products used. The information is collected when an account is opened, but it is infrequently updated. These inputs, along with the weighting each is given, are used to calculate a risk-rating score. But the scores are notoriously inaccurate, not only failing to detect some high-risk customers, but often misclassifying thousands of low-risk customers as high risk. This forces institutions to review vast numbers of cases unnecessarily, which in turn drives up their costs, annoys many low-risk customers because of the extra scrutiny, and dilutes the effectiveness of anti-money laundering (AML) efforts as resources are concentrated in the wrong place.

In the past, financial institutions have hesitated to do things differently, uncertain how regulators might respond. Yet regulators around the world are now encouraging innovative approaches to combat money laundering and leading banks are responding by testing prototype versions of new processes and practices.[3] Some of those leaders have adopted the approach to customer risk rating described in this article, which integrates aspects of two other important AML tools: transaction monitoring and customer screening. The approach identifies high-risk customers far more effectively than the method used by most financial institutions today, in some cases reducing the number of incorrectly labeled high-risk customers by between 25 and 50 percent. It also uses AML resources far more efficiently.

### Best practices in customer risk rating

To adopt the new generation of customer risk-rating models, financial institutions are applying five best practices: they simplify the architecture of their models, improve the quality of their data, introduce statistical analysis to complement expert judgement, continuously update customer profiles while also considering customer behavior, and deploy machine learning and network science tools.

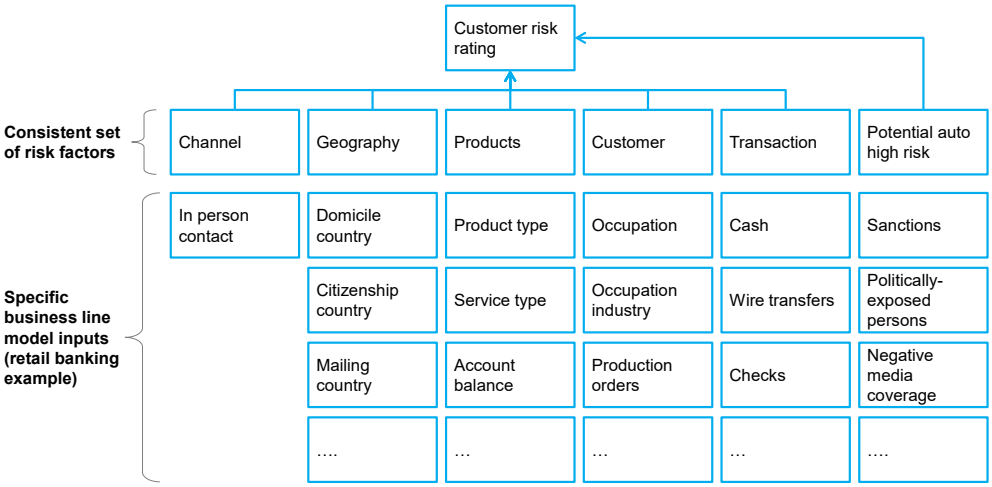
1 "Money-laundering and globalization," United Nations Office on Drugs and Crime, unodc.org
2 Gavin Finch, "World's biggest banks fined $321 billion since financial crisis," Bloomberg, March 2, 2017, bloomberg.com
3 The US Treasury and banking agencies have together encouraged innovative anti–money laundering (AML) practices; see "Agencies issue a joint statement on innovative industry approaches," US Office of the Comptroller of the Currency, December 3, 2018, occ.gov. In China, the Hong Kong Monetary Authority has backed the wider use of regulatory technology, and in the United Kingdom, the financial regulator has established a fintech sandbox to test AML innovations

### 1. Simplify the model architecture

Most AML models are overly complex. The factors used to measure customer risk have evolved and multiplied in response to regulatory requirements and perceptions of customer risk but still are not comprehensive. Models often contain risk factors that fail to distinguish between high- and low-risk countries, for example. In addition, methodologies for assessing risk vary by line of business and model. Different risk factors might be used for different customer segments, and even when the same factor is used it is often in name only. Different lines of business might use different occupational risk-rating scales, for instance. All this impairs the accuracy of risk scores and raises the cost of maintaining the models. Furthermore, a web of legacy and overlapping factors can make it difficult to ensure that important rules are effectively implemented. A person exposed to political risk might slip through screening processes if different business units use different checklists, for example.

Under the new approach, leading institutions examine their AML programs holistically, first aligning all models to a consistent set of risk factors, then determining the specific inputs that are relevant for each line of business *(Exhibit 1)*. The approach not only identifies risk more effectively but does so more efficiently, as different businesses can share the investments needed to develop tools, approaches, standards, and data pipelines.

**Exhibit 1.** Effective, efficient risk-rating models use a consistent set of risk factors, although inputs will vary by business line.




### 2. Improve data quality

Poor data quality is the single biggest contributor to the poor performance of customer risk-rating models. Incorrect know-your-customer (KYC) information, missing information on company suppliers, and erroneous business descriptions impair the effectiveness of screening tools and needlessly raise the workload of investigation teams. In many institutions, over half the cases reviewed have been labeled high risk simply due to poor data quality.

The problem can be a hard one to solve as the source of poor data is often unclear. Any one of the systems that data passes through, including the process for collecting data, could account for identifying occupations incorrectly, for example. However, machine-learning algorithms can search exhaustively through subsegments of the data to identify where quality issues are concentrated, helping investigators identify and resolve them. Sometimes, natural-language processing (NLP) can help. One bank discovered that a great many cases were flagged as high risk and had to be reviewed because customers described themselves as a doctor or MD, when the system only recognized “physician” as an occupation. NLP algorithms were used to conduct semantic analysis and quickly fix the problem, helping to reduce the

enhanced due-diligence backlog by more than 10 percent. In the longer term, however, better-quality data is the solution.

**3. Complement expert judgment with statistical analysis**

Financial institutions have traditionally relied on experts, as well as regulatory guidance, to identify the inputs used in risk-rating-score models and decide how to weight them. But different inputs from different experts contribute to unnecessary complexity and many bespoke rules. Moreover, because risk scores depend in large measure on the experts' professional experience, checking their relevance or accuracy can be difficult. Statistically calibrated models tend to be simpler. And, importantly, they are more accurate, generating significantly fewer false-positive high-risk cases.

Building a statistically calibrated model might seem a difficult task given the limited amount of data available concerning actual money-laundering cases. In the United States, suspicious cases are passed to government authorities that will not confirm whether the customer has laundered money. But high-risk cases can be used to train a model instead. A file review by investigators can help label an appropriate number of cases—perhaps 1,000—as high or low risk based on their own risk assessment. This data set can then be used to calibrate the parameters in a model by using statistical techniques such as regression. It is critical that the sample reviewed by investigators contains enough high-risk cases and that the rating is peer-reviewed to mitigate any bias.

Experts still play an important role in model development, therefore. They are best qualified to identify the risk factors that a model requires as a starting point. And they can spot spurious inputs that might result from statistical analysis alone. However, statistical algorithms specify optimal weightings for each risk factor, provide a fact base for removing inputs that are not informative, and simplify the model by, for example, removing correlated model inputs.

**4. Continuously update customer profiles while also considering behavior**

Most customer risk-rating models today take a static view of a customer's profile—his or her current residence or occupation, for example. However, the information in a profile can become quickly outdated: most banks rely on customers to update their own information, which they do infrequently at best. A more effective risk-rating model updates customer information continuously, flagging a change of address to a high-risk country, for example. A further issue with profiles in general is that they are of limited value unless institutions are also considering a person's behavior as well. We have found that simply knowing a customer's occupation or the banking products they use, for example, does not necessarily add predictive value to a model. More telling is whether the customer's transaction behavior is in line with what would be expected given a stated occupation, or how the customer uses a product.

Take checking accounts. These are regarded as a risk factor, as they are used for cash deposits. But most banking customers have a checking account. So, while product risk is an important factor to consider, so too are behavioral variables. Evidence shows that customers with deeper banking relationships tend to be lower risk, which means customers with a checking account as well as other products are less likely to be high risk. The number of in-person visits to a bank might also help determine more accurately whether a customer with a checking account posed a high risk, as would his or her transaction behavior—the number and value of cash transactions and any cross-border activity. Connecting the insights from transaction-monitoring models with customer risk-rating models can significantly improve the effectiveness of the latter.

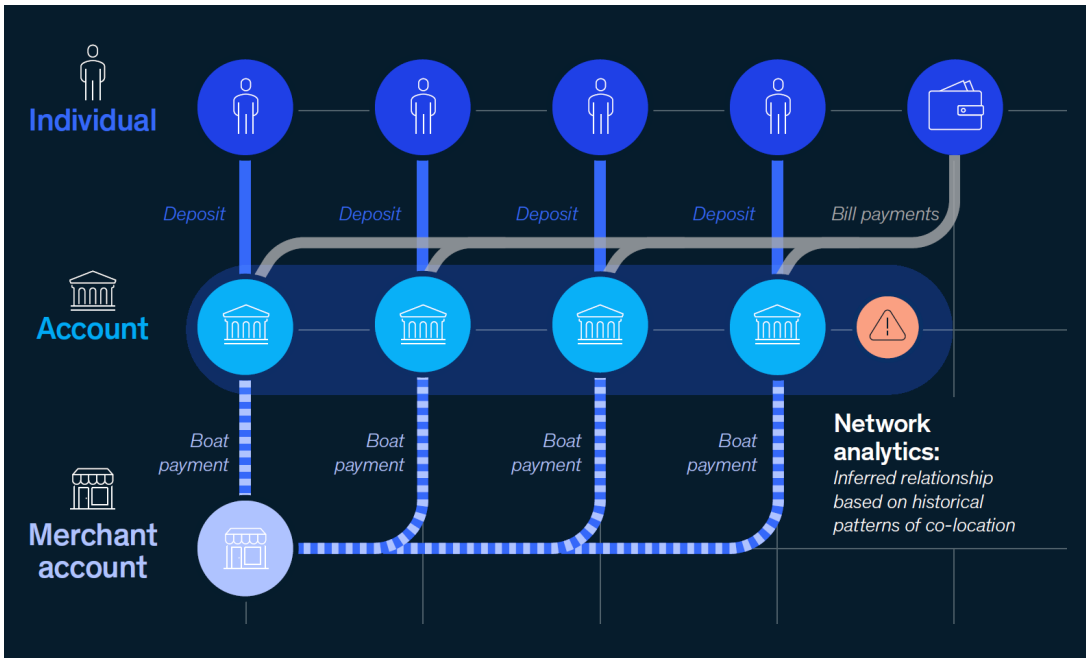
**5. Deploy machine learning and network science tools**

While statistically calibrated risk-rating models perform better than manually calibrated ones, machine learning and network science can further improve performance.

The list of possible model inputs is long, and many on the list are highly correlated and correspond to risk in varying degrees. Machine-learning tools can analyze all this. Feature-selection algorithms that are assumption-free can review thousands of potential model inputs to help identify the most relevant features, while variable clustering can remove redundant model inputs. Predictive algorithms (decision trees and adaptive boosting, for example) can help reveal the most predictive risk factors and combined indicators of high-risk customers—perhaps those with just one product, who do not pay bills but who transfer round-figure dollar sums internationally. In addition, machine-learning approaches can build competitive benchmark models to test model accuracy, and, as mentioned above, they can help fix data-quality issues.

Network science is also emerging as a powerful tool. Here, internal and external data are combined to reveal networks that, when aligned to known high-risk typologies, can be used as model inputs. For example, a bank's usual AML monitoring process would not pick up connections between four or five accounts steadily accruing small, irregular deposits that are then wired to a merchant account for the purchase of an asset—a boat perhaps. The individual activity does not raise alarm bells. Different customers could simply be purchasing boats from the same merchant. Add in more data however—GPS coordinates of commonly used ATMs for instance—and the transactions start to look suspicious because of the connections between the accounts *(Exhibit 2)*. This type of analysis could discover new, important inputs for risk-rating models. In this instance, it might be a network risk score that measures the risk of transaction structuring—that is, the regular transfer of small amounts intended to avoid transaction-monitoring thresholds.

**Exhibit 2.** Network science can reveal suspicious connections between apparently discrete accounts.

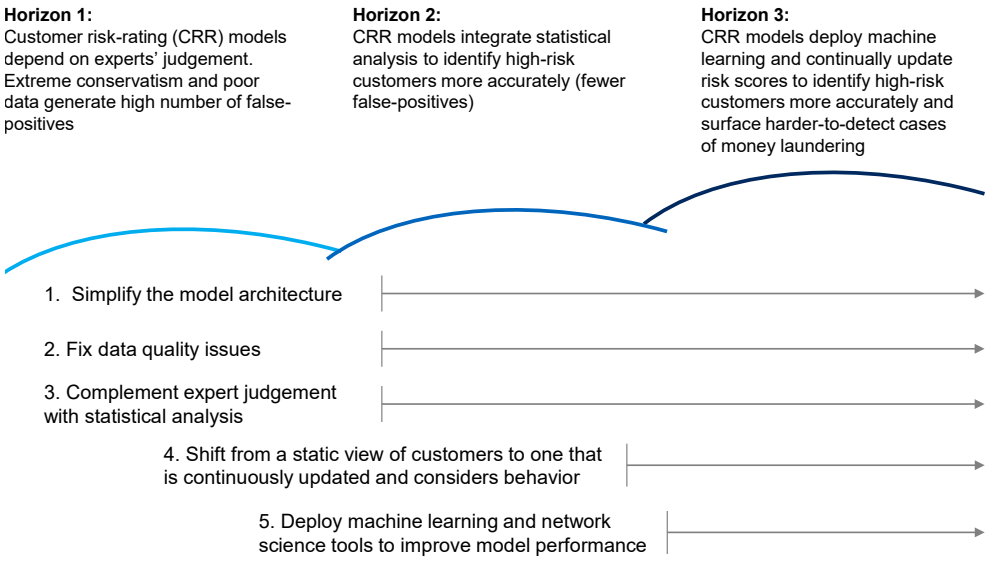


Although such approaches can be powerful, it is important that models remain transparent. Investigators need to understand the reasoning behind a model's decisions and ensure it is not biased against certain groups of customers. Many institutions are experimenting with machine-based approaches combined with transparency techniques such as LIME or Shapley values that explain why the model classifies customers as high risk.

## Moving ahead

Some banks have already introduced many of the five best practices. Others have further to go. We see three horizons in the maturity of customer risk-rating models and, hence, their effectiveness and efficiency *(Exhibit 3)*.

**Exhibit 3.** Moving along the three horizons, the model becomes more sophisticated and thus greater in its effectiveness and efficiency.




Most banks are currently on horizon one, using models that are manually calibrated and give a periodic snapshot of the customer's profile. On horizon two, statistical models use customer information that is regularly updated to rate customer risk more accurately. Horizon three is more sophisticated still. To complement information from customers' profiles, institutions use network analytics to construct a behavioral view of how money moves around their customers' accounts. Customer risk scores are computed via machine-learning approaches utilizing transparency techniques to explain the scores and accelerate investigations. And customer data are updated continuously while external data, such as property records, are used to flag potential data-quality issues and prioritize remediation.

Financial institutions can take practical steps to start their journey toward horizon three, a process that may take anywhere from 12 to 36 months to complete (see sidebar, "The journey toward sophisticated risk-rating models").

## The journey toward sophisticated risk-rating models

**Getting started: How to move from horizon one to two**

— Assemble a team of experts from compliance, business, data science, and technology and data.

— Establish a common hierarchy of risk factors informed by regulatory guidance, experts, and risks identified in the past.

— Start in bite-size chunks: pick an important model to recalibrate that the team can use to develop a repeatable process.

— Assemble a file-review team to label a sample of cases as high or low risk based on their own risk assessment. Bias the sample to ensure that high-risk cases are present in sufficient numbers to train a model.

— Use a fast-paced and iterative approach to cycle through model inputs quickly and identify those that align best with the overarching risk factors. Be sure there are several inputs for each factor.

— Engage model risk-management and technology teams early and set up checkpoints to avoid any surprises.

**Becoming an industry leader: How to move from horizon two to three**

— Begin to build capabilities in machine learning, network science, and natural-language processing by hiring new experts or identifying potential internal transfers.

— Construct a network view of all customers, initially building links based on internal data and then creating inferred links. This will become a core data asset.

— Set up a working group to identify technology changes that can be deployed on existing technology (classical machine learning may be easier to deploy than deep learning, for example) and those that will require longer-term planning.

— Design and implement customer journeys in a way that facilitates quick updates to customer data. An in-person visit to a branch should always prompt a profile update, for example. Set up an innovation team to continuously monitor model performance and identify emerging high-risk typologies to incorporate into model calibration.

□ □ □

As the modus operandi for money launderers becomes more sophisticated and their crimes more costly, financial institutions must fight back with innovative countermeasures. Among the most effective weapons available are advanced risk-rating models. These more accurately flag suspicious actors and activities, applying machine learning and statistical analysis to better-quality data and dynamic profiles of customers and their behavior. Such models can dramatically reduce false positives and enable the concentration of resources where they will have the greatest AML effect. Financial institutions undertaking to develop these models to maturity will need to devote the time and resources needed for an effort of one to three years, depending on each institution's starting point. However, this is a journey that most institutions and their employees will be keen to embark upon, given that it will make it harder for criminals to launder money.

**Daniel Mikkelsen** is a senior partner in McKinsey's London office, **Azra Pravdic** is an associate partner in the Brussels office, and **Bryan Richardson** is a senior expert in the Vancouver office.

# Making your KYC remediation efforts risk and value-based

**Banks are sitting on large know-your-customer (KYC) and due diligence backlogs. Four steps can cut them quickly and improve the customer experience by ensuring remediation efforts are better aligned with business value and the potential risks each customer poses.**

Mette Gade, Daniel Mikkelsen, and Dan Williams

Banks worldwide have paid over $30 billion in penalties since 2009 for failing to crack down on financial crime. Add to that the reputational cost of getting embroiled in money laundering scandals and it's not hard to see why banks are so keen to meet anti-money laundering (AML) requirements. Yet many are overwhelmed by the very first steps of the process, finding themselves sitting on large know-your-customer (KYC) and due diligence backlogs.

Why? Firstly because of the scale of the task. Collecting, validating and continually updating data for millions of customers is time consuming, and frequently changing requirements means that approaches to KYC needs to be rethought. In addition, there are plenty of inefficiencies in the process, which remains largely manual to this day. Previously-recorded information is buried in various paper or electronic files, proving hard to access and aggregate. Queries ping pong back and forth between customers, frontline and back-office staff. Customer insights and lessons learned during due diligence aren't taken into account in monitoring activities or when setting controls.

It needn't be like this. The same 'digital first' approach that has transformed banks' commercial and operational performance with digital technology and agile methodologies can similarly transform KYC and due diligence. Here are four steps that can quickly cut the backlog, improve the customer experience and, importantly, shift the focus to optimizing value while mitigating risks.

## Four steps to ensure a risk-based KYC and due diligence remediation

1. To manage both risk *and* value, segment customers more finely. Most banks expend disproportionate effort on customers who pose very little or no risk.
2. Deploy self-service solutions that are risk-sensitive and carry minimal execution costs. Self-service should be the default option for customers providing KYC information. By automatically posing more questions to customers whose responses suggest higher risk, the burden on less-risky customers is kept to a minimum.
3. Tailor and track remediation efforts at the individual customer level. This will inform required actions and provide operations, the board and regulators a clear view of how remediation efforts are faring.
4. To quicken progress, make use of third-party data, external providers and artificial intelligence (AI). There are plenty of off-the-shelf solutions and data providers that can help quickly stitch together an integrated solution. AI can then accelerate learnings from these outputs.

## 1. To manage both risk *and* value, segment customers more finely

Existing AML customer risk-rating models will likely identify between 0 and 5 percent of customers as potentially high risk-although in some banking segments this proportion can be higher. These customers

are prioritized and undergo enhanced due diligence. The remaining 90-plus percent, however, are grouped into two or three segments, or occasionally only one. As a result, most customers undergo similar or barely differentiated levels of KYC and due diligence, with banks often devoting unnecessary resources on the majority of their customers posing minimal or no risk.

A model that segments customers more finely – perhaps into as many as 10 to 30 categories – can ensure remediation efforts are aligned with the level of risk. Building one takes time, however. In the interim, consider a pragmatic approach in keeping with agile principles that strive for incremental improvements and fast learning, using available customer information. For example, customers who only have a deposit account, have pension products, whose transactions are below a certain threshold or whose accounts are inactive, typically pose limited risks. As many as 75 percent of customers may fall into this category. On the other hand, customers who use a range of digital channels or have used a digital channel for onboarding and lack in-person identity verification would fall into a higher priority category.

Often, in-house customer data can be supplemented with external data. Take, for example, knowledge that a customer is a student. One bank used public records on the average wealth of university students in different regions to understand "normal" wealth and banking activity for these customers, enabling IT to categorize most into a lower-risk category.

This finer segmentation can be used to set appropriate remediation activities, choosing between proactive or reactive contact with customers, for example, and determining various monitoring procedures and controls, such as an automatic alert if a customer moves into a riskier category. Segmentation can also address some regulatory priorities, such as understanding the expected banking activity and source of wealth of a customer, using available data, without the need to ask the customer.

## 2. Deploy self-service solutions that are risk sensitive and carry minimal execution costs

To lighten banks' workload, a full self-service solution should be the default option for customers undergoing KYC and due diligence in high volume segments – that is, retail banking, small corporates and, potentially, high wealth customers. Self-service can reduce marginal execution costs to near zero. Because some customers will need assistance, the solution should be configured so that staff can access it as well, whether to help customers stuck on a certain question or requesting full assistance. Alternatively, staff can contact customers to gather preliminary information, then ask them to complete the process online.

Importantly, self-service solutions should be risk-sensitive, automatically increasing the number of questions proportionate to a customer profile's implied risk. This eases the burden on low-risk customers, ensures the proper information is collected for higher risk customers, and quickly highlights areas where manual intervention may be required.

Self-service solutions will not be perfect from the outset – which is why they must be configured so that improvements can be rapidly implemented. One bank found customers stumbled over a question requiring a tax identification number. Quick rewording solved the problem in minutes – something that would have taken a month or more in a typical IT release process.

For customers who prefer to visit a branch or speak on the phone to complete the KYC process, bear in mind that the necessary conversations around spending patterns and sources of wealth also provide an opportunity to offer advice on other products and services, such as investment planning, pension products, and mortgage re-financing.

## 3. Tailor and track the remediation efforts at the individual customer-level

Remediation efforts will be more powerful if teams follow the approach used by digital marketers. Would-be customers' online progress is digitally tracked through a "sales funnel", helping marketers learn where and how best to intervene to keep them moving from the initial consideration of a purchase through to a sale.

In the same way, banks can track each customer's progress though the KYC and due diligence process, determining appropriate actions at each stage depending on the customer's preferences, behavioral profile and risk categorization. In marketing language, each customer is a segment of one. For example, an automated pop-up reminder to submit information in a mobile banking app might suffice for many customers. But some may need a second message emphasizing the importance of countering financial crime, and still others a third notifying them that their account has been blocked until the information is submitted. Banks may discover that certain customers respond better to a call than an email, or a better time of day at which to reach them.

It will, of course, take time for banks to clear remediation backlogs and become fully compliant. But an agile approach ensures continuous improvement. Therefore, tracking the remediation status of each segment, expected completion of the remediation and required escalations and sanctions is essential. Make sure progress in meeting timelines and any lessons learned are clear to all. Only then will teams be able to improve the remediation process, and executive management gain comfort with it. Importantly, this transparency also broadens discussions with boards and regulators from a singular focus on whether deadlines have been met to one that also considers whether the highest risks are being appropriately addressed.

## 4. To quicken progress, make use of third-party data, external providers and artificial intelligence (AI)

In addition to using the vast amount of internal data for pre-population or validation, plenty of help is available for getting the data you need. RegTechs and other providers can provide lists of beneficial owners, politically-exposed persons (PEPs), or those who feature negatively in media coverage. Public registries and utilities can, in some countries, supply tax and salary records. And don't overlook data generated from customers' digital footprints, if local regulations allow and customers consent, or location data that can verify a customer's presence close to a given address.

AI, meanwhile, will not only speed the KYC and due diligence process, but help to improve it continuously. Optical character recognition (OCR), for example, can extract information from old customer records for validation or pre-population. Fuzzy logic can reduce the number of false positives generated when customers or colleagues make typing errors. AI can also ensure that learnings from transaction monitoring or false positives are used to refine initial KYC questions, optimizing not just the KYC process but the full AML value chain.

While the mindset should shift to "digital first," some manual intervention will still be needed. Make good use of smart workflow tools to ease case handling, as their numbers are growing. The best AML value chains are typically those that stitch together the best platform providers and efficient AI engines for continuous learning loops. No single vendor provides everything you need.

Ultimately, the most important AML value chains may prove to be those established by banks and financial institutions to pool their resources in an AML utility. The aim is not only to share technology costs, but to derive more powerful insights from collective data and crack down harder on financial crime.

□ □ □

**Mette Gade** is an associate partner in McKinsey's Copenhagen office, **Daniel Mikkelsen** is a senior partner in McKinsey's London office, and **Dan Williams** is a partner in McKinsey's Washington DC office.

# Network analytics and the fight against money laundering

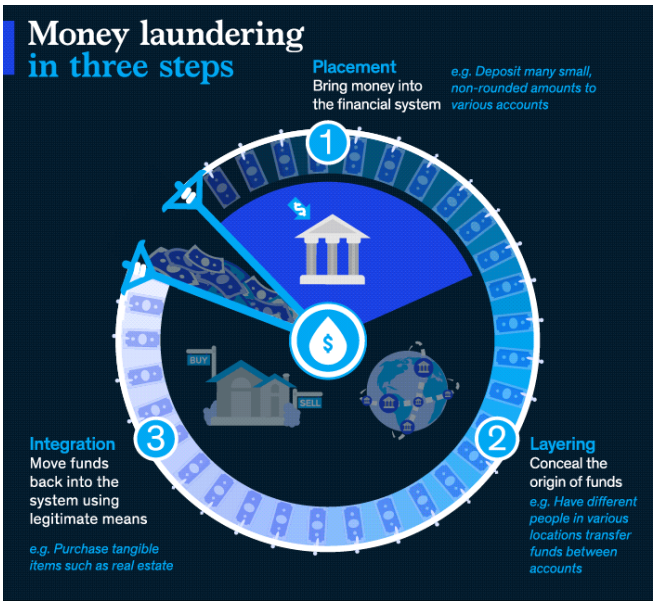
**Network analytics has the potential to significantly improve the effectiveness of AML programs. But banks need the right external data sources and network science capabilities, and deep subject matter expertise, to get the benefits.**

Bryan Richardson, Dan Williams, and Daniel Mikkelsen

Money laundering transforms profits from illegal activities—such as fraud, drug and human trafficking, organized crime, and corruption—into seemingly legitimate earnings by concealing the source of the acquired funds.

Recent estimates show that approximately $800 billion to $2 trillion is laundered annually through the global banking system. That's roughly 2 to 5 percent of global GDP. In recognition of the growing problem, regulators are developing stricter policies—and handing out heftier fines when institutions are caught laundering money.

This is a significant problem for many financial institutions, as those laundering money use increasingly sophisticated methods to evade detection. Although banks are typically on the front lines, other industries used to conceal the source of funds include academia, real estate, hospitality, and healthcare.




## Anti-money laundering (AML) mitigates the flow of illegal funds

Traditional AML performed by a bank uses a customer's profile and transaction history to generate risk ratings and flag various suspicious behavior, such as cash deposits over $10,000. This rules-based approach is critical, but it doesn't account for funds laundered through networks of individuals in smaller, non-rounded dollar amounts to avoid detection.

As a result, customer-risk rating and transaction monitoring models used by banks often exhibit false positive rates of over 98 percent. Although this evidences a conservative approach that may be appreciated by regulators, it can have the effect of diverting resources away from the highest-risk cases.

In appreciation of these growing challenges in AML, regulators have signaled that they are open to banks developing innovative methods to stay ahead of today's tech-savvy criminals. Many leading institutions are exploring the use of natural language processing, network analytics, and other machine-learning and AI-based techniques to identify subtle indicators of illicit activity.

## Network analytics in the real world

Network analytics examines the connections between related entities to better illuminate relationships. Instead of analyzing an individual, subcomponents of the network are reviewed for similarity to known methods of money laundering and atypical customer behavior.

Networks are formed by links between customers and related activity. These (sometimes inferred) links can be internal data, such as account transfers or joint ownership, or external data, such as a shared address or common use of the same ATM.

Network analytics compliments existing machine learning and fuzzy logic-based approaches that many banks use for AML monitoring. Network statistics (for example, connectivity) for each customer can be used as an input to improve the accuracy of customer risk rating or transaction monitoring models. Fuzzy logic-based approaches that resolve customer identities can also be improved by looking at how closely accounts are connected. In addition to improving the effectiveness of existing techniques, network analytics provides investigators with new capabilities. For example, community detection algorithms can identify the presence of customer groups that could be indicative of criminal behavior.

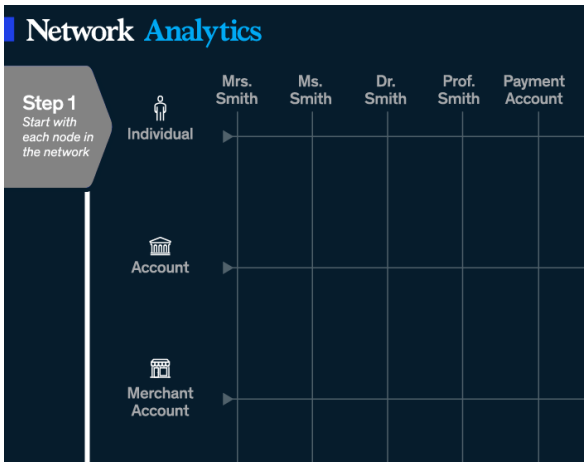
For example: The Smith family is laundering money by dividing large transactions into small deposits, filtered through online bill payments into temporary accounts. The payments are then used to purchase a boat which is quickly resold for cash—creating a paper trail to clean the money.

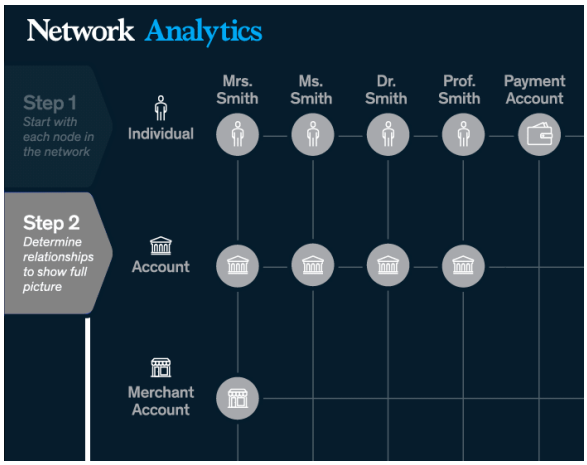
Network analytics can help identify the Smith family's illegal activities. Here's how it works:

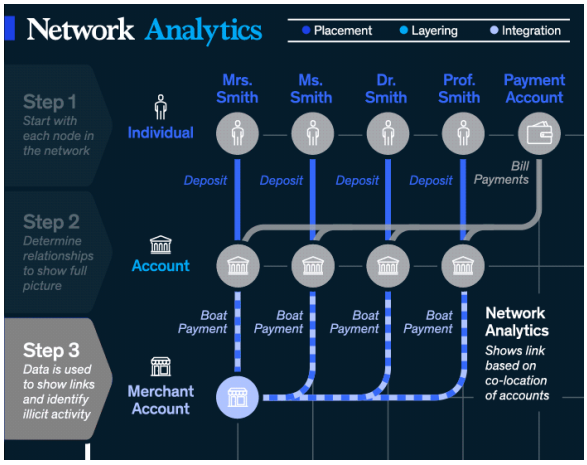
**Step 1: Build the Smith network**
Begin with Mrs. Smith and identify all other entities, including accounts and people, that she is connected to.

**Step 2: Create connections**
Next, add the relationships between the individuals, their respective accounts, and any related activity showing payments made within the system to show the flow of funds.

**Step 3: Infer relationships using non-traditional data sources**
Use enriched data about individuals and their related accounts in order to uncover inferred connections that show suspicious or anomalous activity that might suggest money laundering.



## Network analytics is the future of AML

Network analytics has the potential to significantly improve the effectiveness of AML programs. In practice, statistics from a network (for example, how closely it resembles a known money-laundering typology) would be incorporated into existing customer-risk rating and transaction monitoring models as inputs to improve model accuracy. New capabilities such as community detection would help accelerate investigations and identify hidden risks.

Network analytics takes time to get right and can require an enormous amount of computational power to sift through all current and past customer relationships. Historically, uniquely identifying a customer across systems to build links was also quite difficult. But this has changed over the past three to five years as banks have invested heavily in data infrastructure and built unique customer identifiers that are shared across systems. Scalable infrastructure (for example, Hadoop, AWS) has also provided institutions with more storage and computational power—enabling new use cases including network analytics.

Start by building a network of existing customer links by using account transfers, shared account ownership, and payments to build linkages both internally and to external institutions using the destination account number. Then create inferred links between customers by looking at shared addresses, employer, or social media data. Although often the target state, an enterprise grade graph database is usually not required—data can be stored in a standard relational database to get started. Even without advanced analytics, creating this database of links will accelerate investigations and provide data scientists with a rich asset that can be used for AML, in addition to a wide variety of other use cases (for example, marketing).

To take full advantage, most institutions will need to build capabilities in network science as the tools may be unfamiliar to even experienced data scientists. This will unlock a significant opportunity to improve both customer risk rating and transaction monitoring. The secrets to success are having the right external data sources and network science capabilities, and using deep subject matter expertise to inform model development.

□ □ □

**Bryan Richardson** is a senior expert in the Vancouver office, **Dan Williams** is a partner in McKinsey's Washington DC office, and **Daniel Mikkelsen** is a senior partner in McKinsey's London office.

# Financial crime and fraud in the age of cybersecurity

## As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

Salim Hasham, Shoan Joshi, and Daniel Mikkelsen

In 2018 the World Economic Forum indicated that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately $8.2 billion on anti–money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever before. In a widely cited estimate, for every dollar of fraud, for example, institutions lose nearly three dollars, once associated costs are added to the fraud loss itself.[1] Risks for banks have risen from diverse factors, including vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, and the greater integration of financial systems within countries and internationally. Cyber crime and malicious hacking have also intensified. In the domain of financial crime, meanwhile, regulators continually revise rules, increasingly to account for illegal trafficking and money laundering, and governments have ratcheted up the use of economic sanctions, targeting countries, public and private entities, and even individuals. Institutions are finding that their existing approaches to fighting such crimes cannot satisfactorily handle the many threats and burdens.

### Financial crime or fraud?

For purposes of detection, interdiction, and prevention, many institutions draw a distinction between fraud and financial crime. Boundaries are blurring, especially since the rise of cyberthreats, which reveal the extent to which criminal activities have become more complex and interrelated. What's more, the distinction is not based on law and regulators sometimes view it as the result of unhelpful organizational siloes. Nevertheless, financial crime has generally meant money laundering and a few other criminal transgressions, including bribery and tax evasion, involving the use of financial services in support of criminal enterprises. It is most often addressed as a compliance issue, as when financial institutions avert fines with anti–money laundering activities. Fraud, on the other hand, generally designates a host of crimes, such as forgery, credit scams, and insider threats, involving deception of financial personnel or services to commit theft. Financial institutions have generally approached fraud as a loss problem, lately applying advanced analytics for detection and even real-time interdiction. Since the advent of cybersecurity threats, however, the distinction has become less relevant, as financial institutions need to use many of the same tools to protect assets against all three categories of crime.

## The evolution of fraud and financial crime

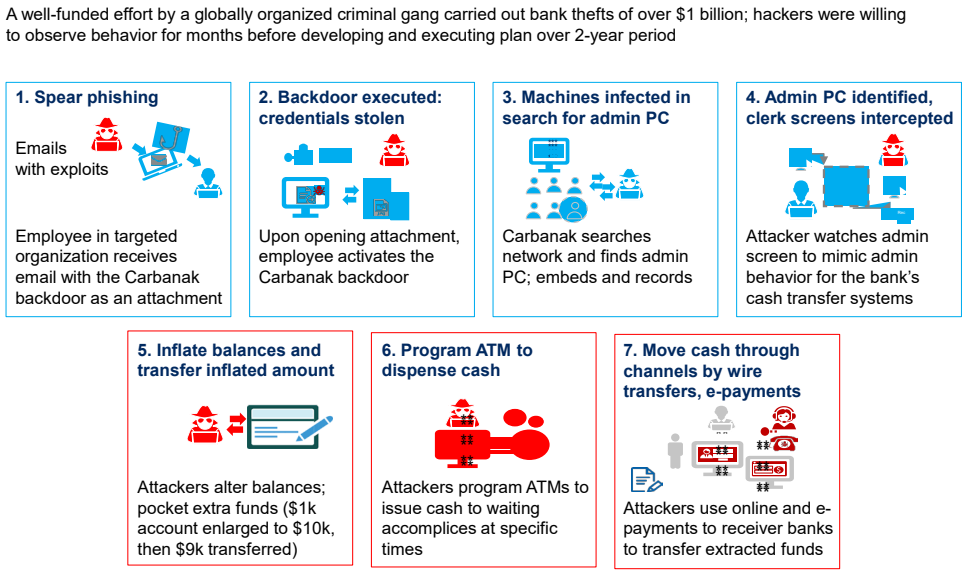
Fraud and financial crime adapt to developments in the domains they plunder. (Most financial institutions draw a distinction between these two types of crimes: for a view on the distinction, or lack thereof, see the sidebar, "Financial crime or fraud?") With the advent of digitization and automation of financial systems, these crimes became more electronically sophisticated and impersonal.

One series of crimes, the so-called Carbanak attacks beginning in 2013, well illustrates the cyber profile of much of present-day financial crime and fraud. These were malware-based bank thefts totaling over

[1] World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; *LexisNexis risk solutions 2018 True Cost of Fraud study,* LexisNexis, August 2018, risk.lexisnexis.com

$1 billion. The attackers, an organized criminal gang, gained access to systems through phishing and then transferred fraudulently inflated balances to their own accounts or programmed ATMs to dispense cash to waiting accomplices *(Exhibit 1)*.

**Exhibit 1.** Financial crime today: the new cyber profile of fraud and financial crime is well-illustrated by the "Carbanak" attacks.



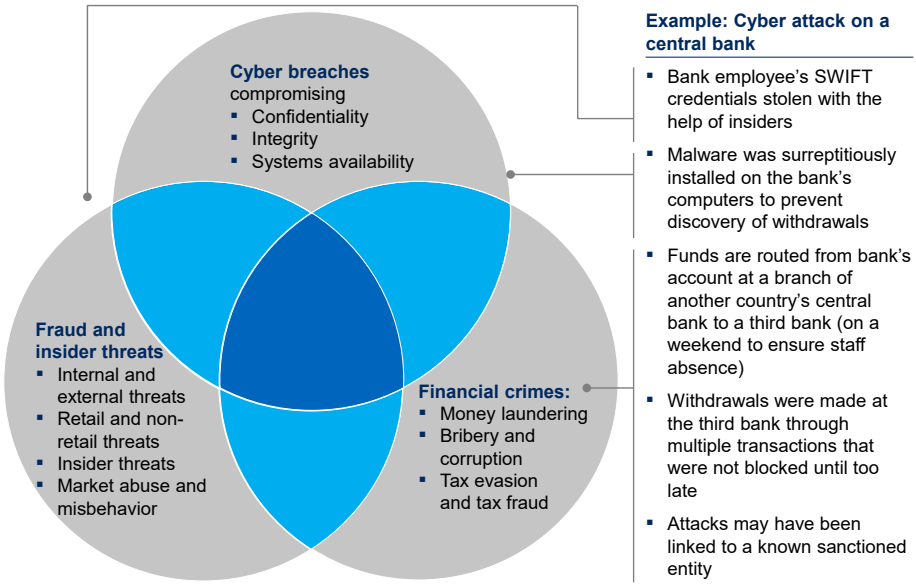

Source: Europol press release, 26 March 2018; *Wired,* 4 April 2018; Kaspersky Lab website

Significantly, this crime was one simultaneous, coordinated attack against many banks. The attackers exhibited a sophisticated knowledge of the cyber environment and likely understood banking processes, controls, and even vulnerabilities arising from siloed organizations and governance. They also made use of several channels, including ATMs, cards, and wire transfers. The attacks revealed that meaningful distinctions between cyberattacks, fraud, and financial crime are disappearing. Banks have not yet addressed the new intersections, which transgress the boundary lines most have erected between the types of crimes *(Exhibit 2)*. A siloed approach to these interconnected risks is becoming increasingly untenable; clearly, the operating model needs to be rethought.

As banks begin to align operations to the shifting profile of financial crime, they first of all confront the deepening connections between cyber breaches and most types of financial crime. The cyber element of these crimes is not new, exactly. Until recently, for example, most fraud has been transaction based, with criminals exploiting weaknesses in controls. Banks counter such fraud with relatively straightforward, channel-specific, point-based controls. Lately, however, identity-based fraud has become more prevalent, as fraudsters develop applications to exploit natural or synthetic data. Cyber-enabled attacks are becoming more ambitious in scope and omnipresent, eroding the value of personal information and security protections.

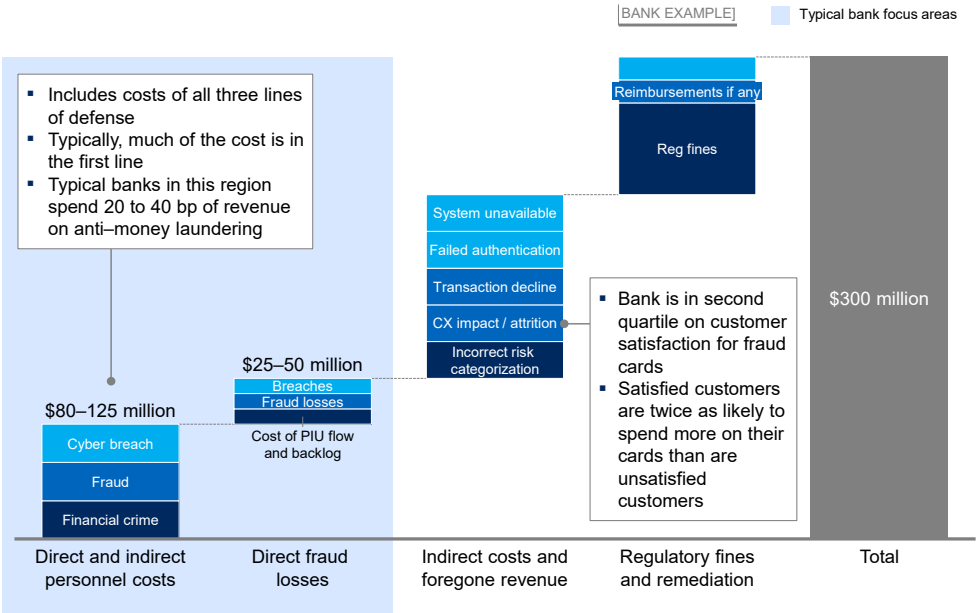
In a world where customers infrequently contact bank staff, but rather interact almost entirely through digital channels, "digital trust" has fast become a significant differentiator for the customer experience. Banks offering a seamless, secure, and speedy digital interface see a positive impact on revenue, while the failure to do this will erode value and lead to lost business. Yet modern banking demands faster risk decisions (such as real-time payments); thus banks must strike the right balance between managing fraud and handling authorized transactions instantly.

**Exhibit 2.** Crime pathways are converging, blurring traditional distinctions between cyber breaches, fraud, and financial crimes.




The growing cost of financial crime and fraud risk has also overshot expectations, pushed upward by several drivers. As banks focus tightly on reducing liabilities and efficiency costs, losses in areas such as customer experience, revenue, reputation, and even regulatory compliance are being missed *(Exhibit 3)*.

**Exhibit 3.** Banks often focus on only a fraction of total financial crime, fraud, and cyber costs.



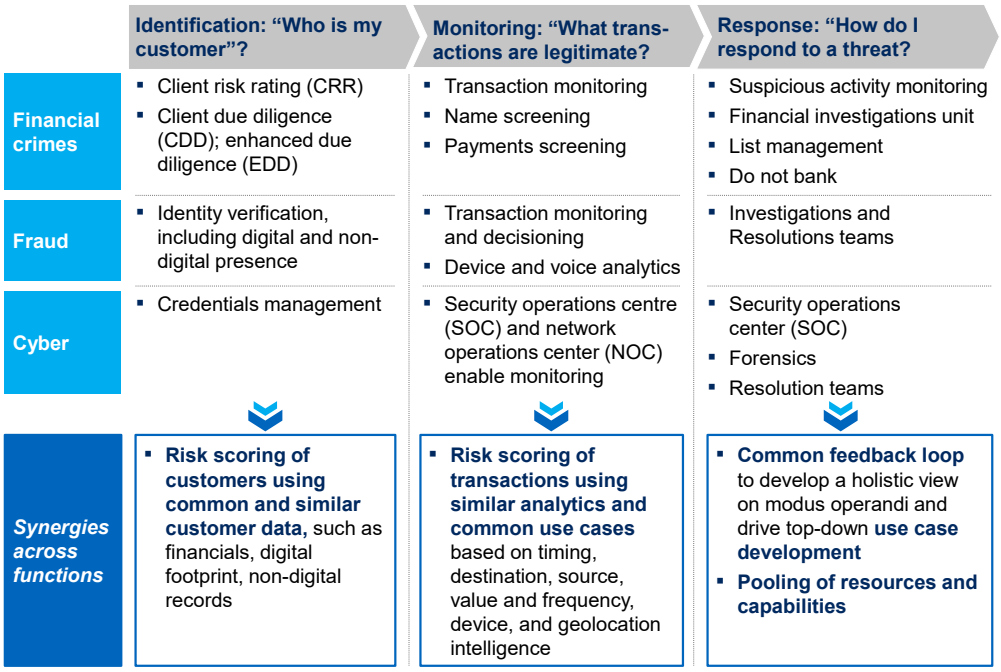
## Bringing together financial crime, fraud, and cyber operations

At leading institutions the push is on to bring together efforts on financial crime, fraud, and cyber crime. Both the front line and operations are oriented in this direction at many banks; recognition is also growing from risk functions and among regulators. AML, while now mainly addressed as a regulatory issue, is seen as being on the next horizon for integration. Key initial steps for institutions embarking on such integration are to define precisely the nature of all related risk-management activities and to clarify the roles and responsibilities across the lines of defense. These steps will ensure complete, clearly delineated coverage—by the businesses and enterprise functions (first line of defense) and by risk, including financial crime, fraud, and cyber operations (second line)—while eliminating duplication of effort.

The truth is that all risks associated with financial crime involve three kinds of countermeasures: identifying and authenticating the customer, monitoring and detecting transaction and behavioral anomalies, and responding to mitigate risks and issues. Each of these activities, whether taken in response to fraud, cybercrime breaches or attacks, or other financial crimes, are supported by many similar data and processes. Indeed, bringing these data sources together with analytics materially improves visibility while providing much deeper insight to improve detection capability; in many instances it also enables a focus on prevention.

In taking a more holistic view of the underlying processes, banks can streamline business and technology architecture to support a better customer experience, improved risk decision making, and greater cost efficiencies. Ideally, institutions will configure their organizations accordingly *(Exhibit 4)*.

**Exhibit 4.** At their core, all functions perform the same three roles using very similar data and processes.

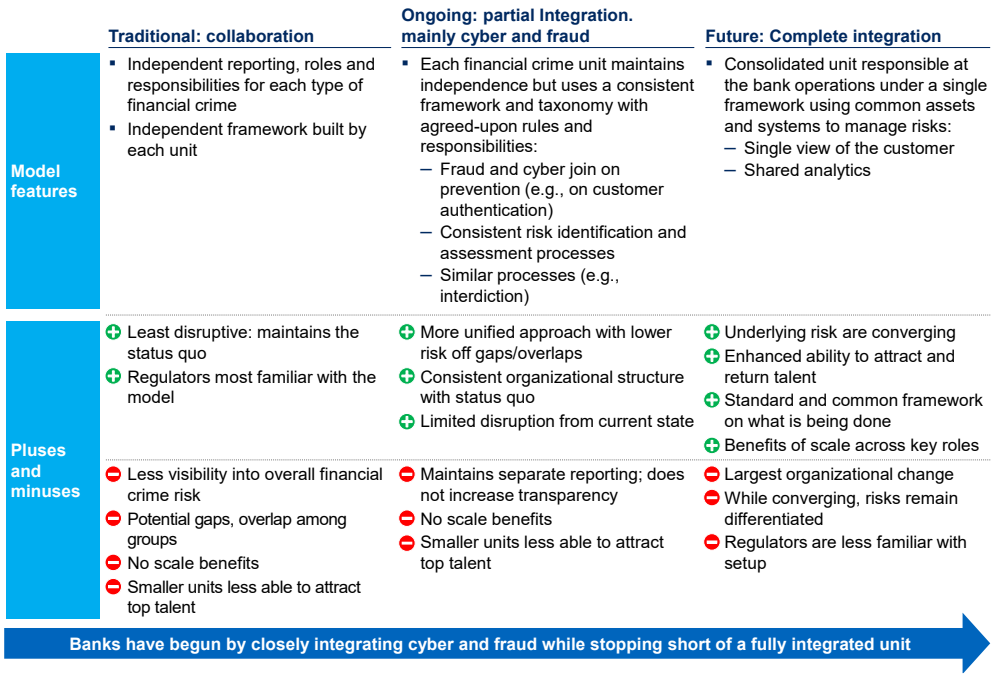



### From collaboration to holistic unification

Three models for addressing financial crime are important for our discussion. They are distinguished by the degree of integration they represent among processes and operations for the different types of crime *(Exhibit 5)*. Generally speaking, experience shows that organizational and governance design are the main considerations in the decision around the operating model. Whatever the particular choice, institutions will need to bring together the right people in agile teams, taking a more holistic approach to common processes

and technologies and doubling down on analytics—potentially creating "fusion centers," to intensify solutions development. It is entirely feasible that an institution will begin with the collaborative model and gradually move toward greater integration, depending on design decisions. We have seen many banks identify partial integration as their target state, with a view that full AML integration is an aspiration.

**Exhibit 5.** Three models for addressing financial crime extend in stages from less to more integrated.




**1. Collaborative model.** In this model, which for most banks represents the status quo, each of the domains—financial crime, fraud, and cyber— maintain their independent roles, responsibilities, and reporting. Each unit builds its own independent framework, cooperating on risk taxonomy and data and analytics for transaction monitoring, fraud, and breaches. Familiar to regulators, the approach offers banks little of the transparency needed to develop a holistic view of financial-crime risk. Further disadvantages are the high potential for coverage gaps or overlaps among the separate groups and the failure to achieve the benefits of scale that come with greater functional integration. The model's reliance on smaller, discrete units also means banks will be less able to attract top leadership talent.

**2. Partially integrated model for cyber and fraud.** Many institutions are now working toward this model, in which cyber and fraud are partially integrated (as the second line of defense). Each unit maintains independence in this model, but works from a consistent framework and taxonomy, following mutually accepted rules and responsibilities. Thus a consistent architecture for prevention (such as for customer authentication) is adopted; risk-identification and assessment processes (including taxonomies) are shared, and similar interdiction processes are deployed. Deeper integral advantages obtain, including consistency in threat monitoring and detection and lower risk of gaps and overlap. The approach remains, however, consistent with the existing organizational structure and little disrupts current operations. Consequently, transparency is not increased, since separate reporting is maintained. No benefits of scale accrue, and as smaller units are maintained, the model is less attractive to top talent.

**3. Unified model.** In this ultimate integrated approach, the financial crimes, fraud, and cybersecurity operations are consolidated into a single framework, with common assets and systems used to manage risk across the enterprise. The model has a single view of the customer and shares analytics. Through risk convergence, enterprise-wide transparency on threats is enhanced, better revealing the most important

underlying risks. The unified model also captures benefits of scale across key roles and thereby enhances the bank's ability to attract and retain top talent. The disadvantage of this model is that it entails significant organizational change. Regulators will therefore be less familiar with bank operations. Despite the organizational change and risk convergence, furthermore, risks remain differentiated.

## The imperative of integration

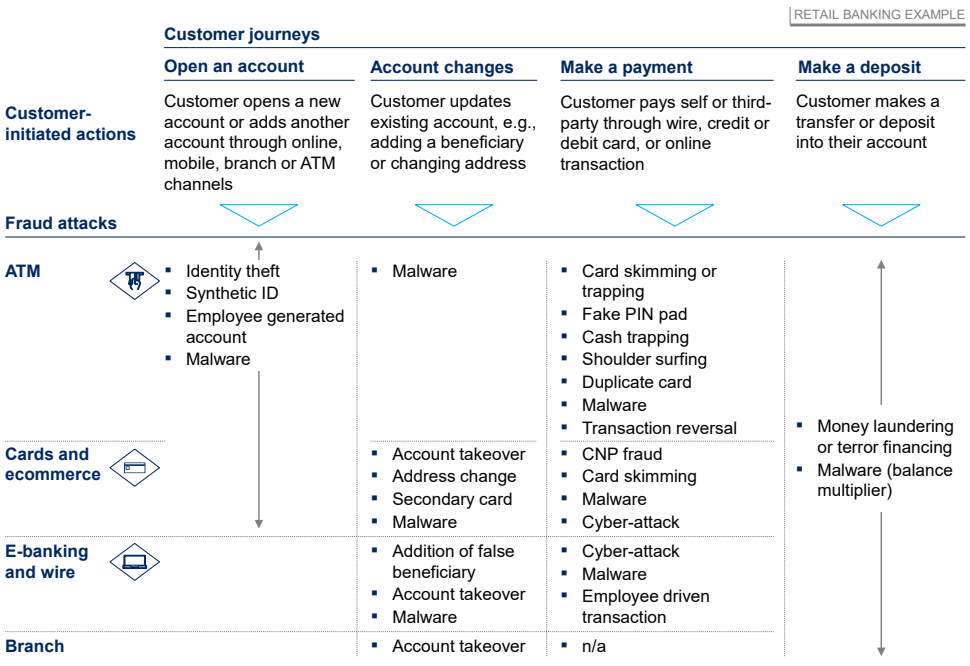
The integration of fraud and cybersecurity operations is an imperative step now, since the crimes themselves are already deeply interrelated. The enhanced data and analytics capabilities that integration enables are now essential tools for the prevention, detection, and mitigation of threats. Most forward-thinking institutions are working toward such integration, creating in stages a more unified model across the domains, based on common processes, tools, and analytics. AML activities can also be integrated, but at a slower pace, with focus on specific overlapping areas first.

The starting point for most banks has been the collaborative model, with cooperation across siloes. Some banks are now shifting from this model to one that integrates cyber and fraud. In the next horizon, a completely integrated model enables comprehensive treatment of cyber security and financial crime, including AML. By degrees, however, increased integration can improve the quality of risk management, as it enhances core effectiveness and efficiency in all channels, markets, and lines of business.

### Strategic prevention: Threats, prediction, and controls

The idea behind strategic prevention is one of prediction of risk rather than reaction to risk. To predict where threats will appear, banks need to redesign customer and internal operations and processes based on a continuous assessment of actual cases of fraud, financial crime, and cyber threats. A view of these is developed according to the customer journey; controls are designed holistically, around processes rather than points. The approach can significantly improve protection of the bank and customers against threats *(Exhibit 6)*.

**Exhibit 6.** With a "customer journey" view of fraud, banks can design controls with the greatest impact.



To arrive at a realistic view of these transgressions, institutions need to adopt a criminal mind-set as it pertains to the business. Crime takes advantage of a system's weak points. Current cyber-crime and fraud defenses are focused on point controls or silos but are not based on an understanding of how criminals actually behave. For example, if banks improve defenses around technology, crime will migrate elsewhere—to call centers, branches, or customers. By adopting this mindset, banks will be able to trace the migratory flow of crime, looking at particular transgressions or types of crime from inception to execution and exfiltration, mapping all the possibilities. By designing controls around this principle, banks are forced to bring together disciplines (such as authentication and voice-stress analysis), which improves both efficacy and effectiveness.

**Efficiencies of scale and processes**

The integrated fraud and cyberrisk functions can improve threat prediction and detection while eliminating duplication of effort and resources. Roles and responsibilities can be clarified so that no gaps are left between functions or within the second line of defense as a whole. Consistent methodologies and processes (including risk taxonomy and risk identification) are directed toward building a consistent understanding and ownership of risks. Institutions can dynamically update the view on the riskiness of clients and transactions by integrating processes and continuously updating risk scores.

**Data, automation, and analytics**

Through integration, the anti-fraud potential of the bank's data, automation, and analytics can be more fully realized. By integrating the data of separate functions from internal and external sources, banks can enhance customer identification and verification. Artificial intelligence and machine learning can also better enable predictive analytics when supported by aggregate sources of information. Insights can be produced rapidly—to establish, for example, correlations between credential attacks, the probability of account takeovers, and criminal money movements. By overlaying such insights on rules-based solutions, banks can reduce the rates of false positives in detection algorithms. This lowers costs and helps investigators stay focused on actual incidents.

The aggregation of customer information that comes from the closer collaboration of the groups addressing financial crime, fraud, and cyber security will generally heighten the power of the institution's analytic and detection capabilities. For example, real-time risk scoring and transaction monitoring to detect transaction fraud can accordingly be deployed to greater effect. This is one of several improvements that will enhance regulatory preparedness by preventing potential regulatory breaches.

**The customer experience and digital trust**

The integrated approach to fraud risk can result in an optimized customer experience. Obviously, meaningful improvements in customer satisfaction help shape customer behavior and enhance business outcomes. In the context of the risk operating model objectives here include the segmentation of fraud and security controls according to customer experience and needs as well as the use of automation and digitization to enhance the customer journey. Survey after survey has affirmed that banks are held in high regard by their customers for performing well on fraud.

Unified risk management for fraud, financial crime, and cyberthreats thus fosters digital trust, a concept that is taking shape as a customer differentiator for banks. Security is clearly at the heart of this concept and is its most important ingredient. However, such factors as convenience, transparency, and control are also important components of digital trust. The weight customers assign to these attributes varies by segment, but very often such advantages as hassle-free authentication or the quick resolution of disputes are indispensable builders of digital trust.

**A holistic view**

The objective of the transformed operating model is a holistic view of the evolving landscape of financial crime. This is the necessary standpoint of efficient and effective fraud-risk management, emphasizing the importance of independent oversight and challenge through duties clearly delineated in the three lines

of defense. Ultimately, institutions will have to integrate business, operations, security, and risk teams for efficient intelligence sharing and collaborative responses to threats. Working together in these ways, the parts of the organization will heighten the effectiveness of independent oversight and challenge through the three lines of defense.

## How to proceed?

When banks design their journeys toward a unified operating model for financial crime, fraud, and cyber, they must probe key questions around processes and activities, people and organization, data and technology, and governance (see sidebar "The target fraud-risk operating model: key questions for banks").

### The target fraud-risk operating model: key questions for banks

In designing their target risk operating model for financial crimes, fraud, and cyber security, leading banks are probing the following questions.

**Processes and activities**

— What are the key processes or activities to be conducted for customer identification and authentication, monitoring and detection of anomalies, and responding to risks or issues?

— How frequently should specific activities be conducted (such as reporting)?

— What activities can be consolidated into a "center of excellence"?

**People and organization**

— Who are the relevant stakeholders in each line of defense?

— What skills and how many people are needed to support the activities?

— What shared activities should be housed together (e.g., in centers of excellence)?

— What is the optimal reporting structure for each type of financial crime (directly to the chief risk officer? to the chief operations officer? to IT?)

**Data, tools, and technologies**

— What data should be shared across cyber, fraud, and other financial crimes divisions? Can the data sit in the same data warehouses to ensure consistency and streamlining of data activities?

— What tools and frameworks should converge (for example, risk-severity matrix, risk-identification rules, taxonomy); how should they converge?

— What systems and applications do each of the divisions use? Can they be streamlined?

**Governance**

— What are the governance bodies for each risk type? How do they overlap? For example, does the same committee oversee fraud and cyber? Does committee membership overlap?

— What are the specific, separate responsibilities of the first line and second lines?

— What measurements are used to set the risk appetite by risk type? How are they communicated to the rest of the organization?

Most banks begin the journey by closely integrating their cyber and fraud units. As they enhance information sharing and coordination across silos, greater risk effectiveness and efficiency becomes possible. In order to achieve the target state they seek, banks are redefining organizational "lines and boxes" but, more importantly the roles, responsibilities, activities, and capabilities required across each line of defense.

Most have stopped short of fully unifying the risk functions relating to financial crimes, though a few have attained a deeper integration. A leading US bank set up a holistic "center of excellence" to enable end-to-end decision making across fraud and cyber. From prevention to investigation and recovery, the bank can point to significant efficiency gains. A global universal bank has even gone all the way, combining all operations related to financial crimes, including fraud and AML, into a single global utility. The bank has attained a more holistic view of customer risk and reduced operating costs by approximately $100 million.

□ □ □

As criminal transgressions in the financial services sector become more sophisticated and break through traditional risk boundaries, banks are watching their various risk functions become more costly and less effective. Leaders are therefore rethinking their approaches to take advantage of the synergies available in integration. Ultimately, fraud, cyber, and AML can be consolidated in a holistic approach based on the same data and processes. Most of the benefits are available in the near term, however, through the integration of fraud and cyber operations.

**Salim Hasham** is a partner in McKinsey's New York office, where **Shoan Joshi** is a senior expert; **Daniel Mikkelsen** is a senior partner in McKinsey's London office.

Transforming approaches to AML and financial crime
September 2019

Designed by US Design Center

www.mckinsey.com

@McKinsey
@McKinsey