

NICE Actimize

White paper

Risk-based Approach for AML and Fraud: Checking the Box is No Longer Viable

We appreciate the high level of engagement during the ACAMS webinar. The NICE Actimize team 2020 ,24 March has compiled additional answers to the questions we were not able to get to during the live Q&A. The selected questions were provided by the audience and were not .supplied by NICE Actimize or ACAMS

NICE Actimize

Contents

COVID-19 4

On-Air Questions 5

Integrated Financial Crime Management 7

Risk Assessments 10

Fraud Management 14

Meet the Experts 15



NICE Actimize

COVID-19

How should organizations handle the increase in alerts that are likely to be generated by COVID-19-prompted large cash withdrawals?

From a fraud perspective, make sure staff understand the potential issues at the point the cash is being handed out. Do correct authentication, ask what it's for, be aware of the current scams and be able to recommend alternative payment methods. Look to amend the rules to generate fewer alerts if there is a concern of very high false positives.

Do we have some relaxation in AML standards because of the COVID issue and lack of support staff?

We have not seen any communications on relaxing the standards due to COVID. Regulators would anticipate that business continuity plans were in place prior to the crisis and enacted when the crisis occurred; however, if certain issues resulted that were not able to be controlled, there may be some leniency. I think this would be on a case-by-case basis and the situation that may have occurred.

Do you think due to COVID-19, fraudsters can take advantage of the situation and how [are they doing this]?

Yes, and they are already. Scams are the key one, with numerous examples already available, such as purchase scams selling fake medication to social engineering asking for bank details to provide government funding. There will also be changes in genuine customer behavior impacting model and rule performance as customers do more digital-based transactions.

With the change in product demand due to the COVID-19 or lack of demand and a change in transactions with businesses, should FIs be preparing to reassess risks for business across their line?

This often happens in adverse times. If you go back several years, the interest rates were at a minimum (okay, they are pretty much today too), but financial institutions had to think outside-the-box on how to book additional revenue. Many of them considered or increased their risk appetite to increase revenue. In that case, you just need to make sure you have plans in place to address the additional risk, and how you are going to monitor it. Look at where the risk is really coming from and put additional controls in place targeted specifically at them.

Considering the unprecedented state of affairs we are currently experiencing and considering most employees are working from home, how important is "Knowing your Employees" vis a vis "Know your Customers" (KYC)? How important is Knowing your Employee from a "fraud point of view"?

It's always important to have undertaken relevant due diligence on employees both at onboarding and on an ongoing basis. With a less visual review of what people are doing, there are larger risks, but these should be built into the employee fraud monitoring and controls. A good employee fraud monitoring system can look for the outliers and anomalies on staff activity.

On-Air Questions

When the financial crimes space is constantly evolving, how do you ensure that your business strategy keeps pace and stays aligned to your risk appetite?

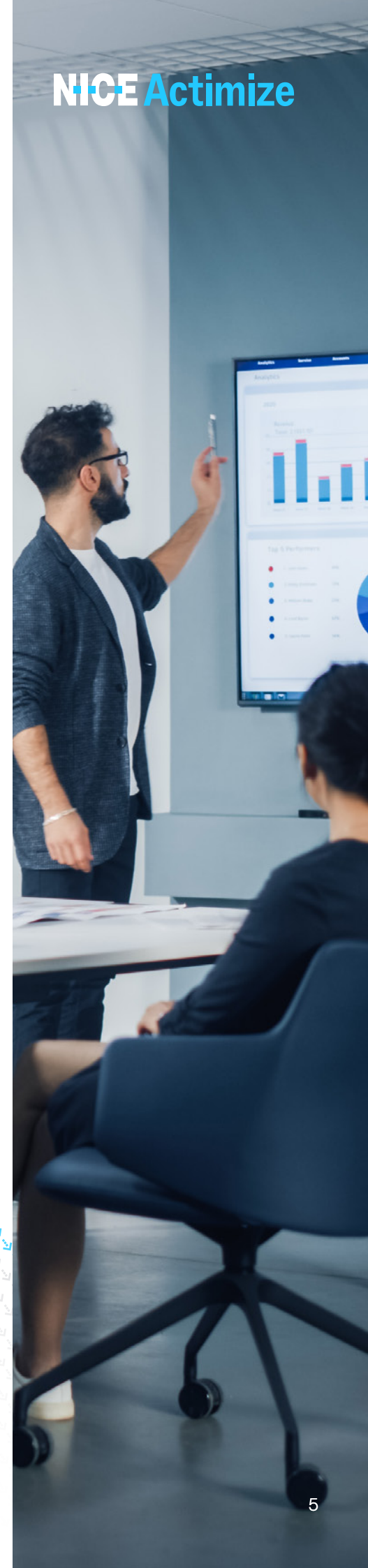
They should be aligned and reviewed together. Organizations need to review the investments in tech and the people required to keep them in tandem, and keep looking a few years out.

However, risk assessment should be developed separately from your risk appetite. The assessment measures the risk while the Risk Appetite is an indicator of the risk you are willing to take on as an organization. If your assessment is tailored to fit your risk appetite, you are compromising your assessment of your client which has farther implications that just comparing to your Risk Appetite. It sets the standard for how you will be monitoring the client and how often you may or may not be doing periodic reviews on them.

How does the increasing regulatory landscape for fraud (OCC, PSD2, CRM) affect taking a risk based approach?

Fraud has traditionally been an area where losses are the "cost of doing business" and need to be accepted to some extent, whereas AML has been about meeting the regulations. The time has come for both to learn from each other. In fraud, we are now seeing increasing regulation coming in such as PSD2 in Europe that mandates fraud profiling and levels of authentication. We are also seeing regs in the UK to force banks on both sides of an authorized fraud transaction to do more to prevent and carry liability.

In the US, the OCC Bulletin 2019-37, brings the need for FS firms to bring in more advanced fraud management practices. While these all limit a riskbased approach to some extent, this is mainly at the extremes. These still allow banks to have a risk appetite and they're choosing to balance fraud against customer experience in most instances. Often it is the banks' level of investment (or lack thereof) that hinders them most.





How do you deal with an organization you are acting for that does not want to implement any additional requirements above from what is required by law or legislation to ensure substance over form?

We need to put it in terms of how investing in this space can bring both regulatory and business benefits. Slicker onboarding can meet and exceed KYC processes, reduce fraud and offer a better customer experience.

Additionally, playing "catch-up" is usually much more costly and in the end, you will end up with a solution that is heavily "band-aided" which also costs more to maintain and upgrade as needed.

With regards to the CDD process - to help prevent getting the CDD wrong, should companies go back and conduct CDD on customers on a recurring basis? If so, to what frequency makes sense? How often is an individual or an entity with little adverse media and, subject to ongoing monitoring, being looked into as part of the risk based approach? How often shall the individual be re-screened..is it every 3 months or lesser?

I would focus more on ensuring the model is correctly classifying your customer base. If you find certain risk factors that are tending to make certain clients higher risk than they should be, you may want to consider adjusting the risk factor. If a change to your CDD model occurs, re-evaluate those customers that would be impacted.

I don't believe a complete review of the entire client base is necessary; however, high-risk clients should be reviewed somewhat regularly. I often see yearly, but I have seen other schedules at every six months or even less in some instances. Medium and low-risk clients could be reviewed less frequently.

NICE Actimize

Integrated Financial Crime Management

Fraud is 80% connected to AML, so why we don't report it to the FIU so they can have it as the whole picture? When funds are transferred fraudulently, they become the proceeds of crime and are therefore being laundered, so this would usually hold true.

When reporting individual transactions to an FIU though, we need to do this in a way that doesn't overload the FIU. The focus should be on adding intelligence, e.g. details of account holders and their devices that were used to undertake the fraud. Often it will be the beneficiary bank that will have some of the best intelligence to share, e.g. the details of the mule and where the funds were subsequently sent. One way to do this is for the data to be shared into a database, rather than individual SARs for each. This means that the links can be found, without being under significant strain. Where required, SARs can be provided covering rings to add intel.

Which term is more important to consider? AML or fraud? How is it in the U.S. and UK?

They are both important and are linked; however, failure on the AML side can lead to very high fines and loss of license to operate. Failure on the fraud side can lead to high losses and loss of customers.

Have you seen any success with financial services cross-training Fraud Ops and AML? How is it benefitting the richness of the investigations?

There is an emerging trend in cross-training Fraud and AML investigations teams and it is also the best practice as cross-training would benefit both the teams to develop overall quality and effectiveness of the investigations and employee morale. In addition to mitigating the risk of inadequate coverage and providing opportunities for learning and advancement, cross-training helps to retain talent as FIs are experiencing high turnover rates within their financial crimes compliance departments.

Would you advise having different teams or have the AML analysts learn how to do fraud investigations?

Having two teams is more ideal, but not always practical depending on the size of the FI. Having one team is okay, as long as you ensure the staff includes some people with AML expertise and some with Fraud expertise, and that you have a path for cross-training. Traditionally, AML analysts have a more compliance-type background whereas Fraud analysts tend to have a stronger operational background. However, a unified case manager helps to bring AML and Fraud personnel together. Much of the data required for AML investigations is the same as that used by Fraud operations. Both use-cases have similar workflows and follow the same approach for case disposition and regulatory reporting. The real benefit comes with having the full transparency of the overall risk on the entity.





Could you please comment if one person could be positioned to MLRO and Fraud officer? Or it is a conflict of interest?

I would not consider this to be a conflict of interest and in some cases with smaller organizations, this is the case. There is an overall financial crimes "owner". If possible, I would recommend having the roles separated as they involve slightly different skillsets; however, it is understood this is not always feasible.

Do you suggest a separate department to conduct an internal investigation? Meaning a Compliance and/or Fraud Officer to review transaction prior to filing reports? What is the ideal way to handle these issues?

Assuming this question is about internal investigation related to employees, it is recommended to have a separate team to be responsible for such investigations. The skills required to conduct internal investigations on employees is different from a typical AML or Fraud investigation. Also, a specialized and isolated group of investigators is preferred because of the sensitivity of employee investigations.

What are the risk and compliance issues for using robotics in the onboarding process?

Studies have shown that CDD/KYC accounts for roughly 60 percent of the AML budget, much of which is related to data collection and other manual tasks. Onboarding is a great place to leverage robotics process automation; however, some controls need to be put in place. If you have automatic processes in place that collect data, regulators are making an assumption that ALL the data that was collected has been reviewed. You want to make sure you don't gather unnecessary data that needs manual reviewing, which would dramatically increase your review times. Also, there should be some type of checkpoints or review to ensure the automated processes are getting the information as expected.

You mentioned benchmarking and a kind of peer analysis related to alert generation and false-positive volumes. Is there a resource for financial institutions to be able to find this information?

Unfortunately, there isn't one industry consolidated repository where this is readily available. There isn't a public consortium either, but NICE Actimize does offer services to perform this benchmarking for their clients.

What KRIs for AML and Fraud management are used as ordinary industry practice? Could you please provide examples?

There is a question later that also talks about key performance indicators as KRIs. I'm making a distinction because KRIs may be referring to key risk indicators as opposed to performance indicators. When we talk about risk indicators, we are generally referring to having strong detection analytics that can identify known fraud and known money-laundering scenarios, as well as suspicious, unusual and anomalous behavior. Good AML and Fraud systems generally have a massive library of this type of risk indicator built-in and use algorithms that weed out the likely criminal issues from the innocent ones. This topic is a big one and best reserved for a dedicated discussion.

What are the current or potential applications of Machine Learning for FIs and regulators?

We need to remember that machine learning is a subset of AI and has been around for quite a long time. In fact, we all practically use applications that leverage machine learning every day. It's also already heavily used in financial institutions already for certain products or services. For financial crimes management, particularly in AML and Fraud, there are many areas it's already in use: segmenting customer populations, optimizing thresholds, anomaly detection, fraud detection, eliminating the noise in data intelligence, prioritizing alerts, optimizing analyst and investigative workloads, and so much more.

How can an analyst apply a risk-based approach for data quality?

I think the author of the question is asking about the governance of data across its life cycle. One thing for certain is that data is important and the adage of "garbage-in" yields "garbage-out" rings true. However, financial crimes systems do rely on having a lot of data, and using AI, will prefer having more data- not less. Machine learning helps to identify what data is actually useful, but you need to provide the data first. Regarding the governance of the data, I suggest you do some research on data governance and data lineage.

Is real-time aggregation of transactions (frontline) for MSBs a regulatory requirement? If so, what specific U.S. regulation?

No, it is not. However, the time is coming for any FI that receives real-time payments to consider monitoring transactions in real time. MS's would be one to benefit from this. As more funds are moved fraudulently on real-time payment rails, the pressure will mount on the beneficiary organizations to do their bit in preventing onward movement. By undertaking Customer Life cycle Risk Management (CLRM), the risk can be reduced by looking for mule risk at onboarding, during ongoing behavior and then actioning in real time when a high-risk inbound payment comes it.

What are the different approaches being taken by different financial crime software vendors?

NICE Actimize combines over 20 years of industry expertise, AI, and the latest technologies built-in to its robust solution to combat financial crime threats. NICE Actimize also includes Collective Intelligence built-in to its default analytics leveraging its consortium-view and supports wide integration to systems and data intelligence. With a unified case manager, FIs have a holistic view of customer risk.

In terms of technology, can you mention some providers that have effective solutions for AML and fraud?

Sure, we invite you to visit NICE Actimize's X-Sight Marketplace here to get an idea of the vast ecosystem of solutions and technologies that can be combined to create an effective financial crime risk and compliance program.





Risk Assessments

Is it feasible to quantify different risks in a representative way during a Risk Assessment process? How can we eliminate the factor of objectivity from the aforementioned RA exercises?

Yes, it is feasible. Risks need to have a probability rating and an impact rating. Multiplying these together can show the overall size of the risk. A good way to review this is to undertake scenario analysis to see if the weightings are accurate and to get other risk teams who are not super experts to challenge.

How often should one review their riskbased framework?

Risk management frameworks do need to be periodically reviewed to ensure continuous improvement. Its purpose is to instill a culture that manages to that risk. Reviewing overall policies and processes should happen regularly, e.g. once a year. However, some policies and rules should be reviewed more often. It's important to document what you say you will do, do what you say you will, and evidence that you have done it. From a fraud perspective, monitoring measures such as valuedetection rate (VDR), false positive rates (FPR) and customer complaints can show where to focus on reviews.

Anti-Money Laundering (AML)

Can you mention on Negative News component?

Assuming you're interested in solutions for negative news, there are many vendor solutions in the industry that offer this capability. Feel free to take a look at the NICE Actimize X-Sight Marketplace as a starting point.

You mentioned performing an independent health check every other year or so. Is this different from the annual independent review? If so, how?

If you are performing an annual independent review, that would probably be equivalent to performing a health check on your models. Some organizations don't have a truly independent review on an annual basis.

What trends do you see the regulators/ examiners focusing on in regards to model validation?

Evidence and independence! The two big things examiners want to see is 1) hard evidence that your model is delivering what you intended and 2) that there was some type of independent validation performed. Third-party validation is always a good idea (either internal or external). Sometimes in the compliance organization, which I was a part of for many years, you tend to be too close to things and can overlook some of the obvious.

How would you consider best integrating 'mitigating factors' in a customer risk scoring?

Today, most customer risk scoring models are considered scorecard models where we add points for certain risk factors and subtract some value for mitigating factors. While not heavily used today, the future of these risk scoring models should adopt AI to use machine learning algorithms to create more accurate views of customer risk and behavior.

What are reasonable levels of KRIs (for example STRs to total operations ratio (%), etc.) for overall medium AML/ CTF risk business? Is there an industry benchmark/metric for SAR production to alert generation? For example, should a bank expect x% of SARs to be generated through model alerts vs. being identified by another means (e.g., review of manual reports, staff notification, etc.)?

There isn't a standard benchmark, but in many discussions, you'll hear that the industry rate is about 95 percent false positives. The term false positives means those alerts didn't result in a SAR, which equates to 5 percent resulting in SARs. I have heard of some organizations that have over 10 percent resulting in SARs and as little as 0.1 percent. You definitely want to increase that number; however, you don't want to "narrow your net" too far that you are missing things and only focusing on the obvious. The other thing to consider is that just because an alert doesn't result in a SAR doesn't mean it is a bad alert. If I deposit 500K into my account and it is non-typical, an alert should occur. If that alert came from the sale of a house, it is closed without a SAR; however, it doesn't mean it was a bad alert, it just needed to be investigated. The alert should have generated.





A lot of high risk customers tend to be larger business customer relationships due to the large amount and volume of their activity. Although it's large in comparison to the population and it's normal not high risk activity, what mitigating factors can be considered to lower the risk of these type customers being flagged as high risk?

My first inclination is to have that customer reviewed with your anti-money laundering oversight committee if their risk level is triggered by one or two factors (i.e. value/volume). If the committee agrees that this is not a high-risk entity, the risk level can be lowered and appropriate documentation captured as to why the risk level was lowered. There may be factors that will make the risk that much less (i.e. publically traded entity). I would also put this on a regular rotation to review with the committee, potentially a one-year review to ensure that they maintain that lower risk. I have seen organizations also suppress certain types of alerts for those organizations and the regulating bodies were in agreement as long as reviews of "that risk" were performed periodically.

Why are we even allowing, knowingly permitting, identified high risk parties to do business with my/your institution? What would be a better choice to protect my/your business operations?

Risk is not always a bad thing, even though many times it is perceived that way. Think of typical investments. There are stable investments and higher risk investments, and the key is finding the right mix for you, much like your organization. When you take on certain risks, you need to identify where the risk lies, in CDD there are probably some factors that identify that. The key is to put in place processes to monitor that risk and alert if there are any abnormalities. You may want to change the scrutiny levels in your transaction monitoring to give less leeway in certain activities for those clients that pose a higher risk. The other, almost mandatory way to do this, is periodic reviews. Set up periodic reviews of those clients to review if anything has changed in their profile, transactional activity, and ensure nothing has surfaced from a piece of negative news or adverse media perspective. Depending on how risky the client is, you may want to lengthen or shorten the time between reviews.

How can an organization mitigate true positive while applying RBA? An example: Suppression of threshold may miss true positive.

First, I would make sure you do enough due diligence up front before putting processes in place that suppress things like alerts. I tend to favor the concept of Hibernation. Hibernation allows you to "set aside" those alerts that have a low probability of turning into a SAR. If in the future, the client/entity has additional hibernated SAR, that is a trigger that you may want to investigate. This gives you visibility into the activity without needing to spend the time investigating.

Which model risk data is most effective in risk ranking clients?

The basics of calculating customer risk fall into three main categories:

- About the customer
- The products and services used
- Geography

Each category has many different risk factors, but there isn't one specific factor that is more effective than the other on a wide scale. It's important to segment your customers appropriately, categorize the risk to your institution's risk appetite, and tune each customer risk model that factors in all of the categories, because they can be drastically different from one to the next.

Is a CDD considered satisfactory, if at the time of onboarding an entity has a member country in a high risk country or possibly sanction, and you have made sure that no individual at senior level is common between both entities? Will this factor pose the slightest risk for onboarding entity?

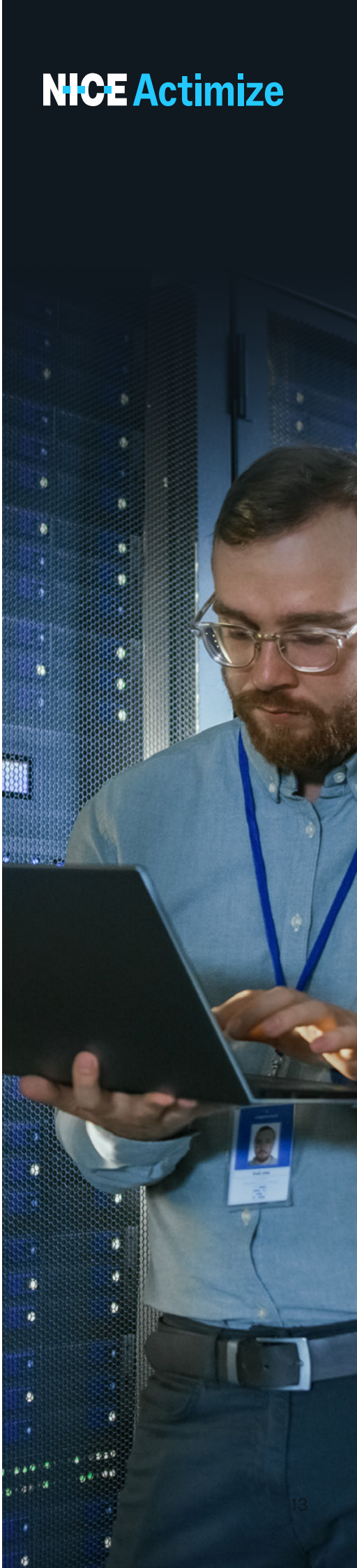
This sounds like a question concerning the onboarding of a multinational corporate entity. And the answer depends on what jurisdiction you are in. When you bring up sanctions, the answer is clear- you cannot do business with the sanctioned entity- so this is obviously risky if the corporation has foreign subsidiaries or affiliates in sanctioned countries. Again, the level of acceptable risk is determined by your institution's risk appetite. Good CDD should factor in all the relationships to the overall assessment of that onboarding entity. In the U.S., the OFAC provides a framework that should be reviewed here.

Regarding FinTechs and AML, new regulations in Brazil starting on July 1, 2020 put a lot of new responsibilities onto AML programs using a risk-based approach. Do you have any tips or general guidelines to inform due your experience?

This is a very loaded question and can't be answered in a few sentences. In general, applying the riskbased approach means you have to clearly identify where your financial crime risks are, apply controls proportionate to the risk to actively manage them, prove that those controls work, and adjust them when appropriate.

How can Artificial Intelligence help banks reduce cost of AML and compliance, and by what percentage?

Well, this is a loaded question! Different vendors claim different percentages for a reduction in costs; however, a more realistic percentage differs on a case-by-case basis. Essentially, your organization should partner with a vendor who will sit down with you to understand your program's current state and the proposed future state. It's at that point when you'll be able to determine a more accurate return on your investment in this type of technology.



Fraud Management



From a fraud perspective, a credit card not present is generally the largest space for losses. What are the key controls to mitigate this risk?

From the card-issuing perspective, there is a need to focus on authentication and fraud profiling. Increased authentication can be brought in using 3DS2.2 to add the ability to do out-of-band authentication to a registered mobile device. This can be done using an authentication model to look for risk in the authentication process and only request the extra authentication where required. Good fraud models look for CNP specifically, taking into account both the issuer and merchant characteristics. Also, the capability to undertake Common Point of Purchase/ Compromise (CPP) analysis along with bringing in external intelligence.

The UK recently announced that contactless payments will be increased to £45 from 1 April; what increased financial crime risk do you see this posing and is there anything firms should be trying to preemptively do?

The increased limit for contactless is a good thing and it would probably go higher if it wasn't limited by the PSD2 rules of 50Eur per individual transaction of a cumulative limit of 150Eur (or five transactions which is a pointless limit). These are very low really, considering that there are other controls that can be in place. Whilse this could lead to some increase in losses per stolen card, this is fairly small. The latest UK Finance figures show that contactless fraud losses increased £1.1 million while the transaction value increased by £11.5 billion. As a percentage of transactions fell from 2.7bps to 2.5bps in 2019, this is comparative to a 15bps loss for eCommerce fraud.

To protect themselves, issuers should have a good monitoring system that can profile customers' usual behavior across payment types to look for those that might be fraud, block cards reported lost/stolen, allow customers to freeze cards in their apps if they think they are lost, and look for unusual behavior at merchants that may highlight fraudulent behavior in one place.

Any major concerns industry wide in regards to SPVs and fraud?

I assume the question refers to Special Purpose Vehicles. SPVs can be used legitimately for many purposes. However, like most things they can be abused. From a fraud point of view, it is best to ask questions like the following to understand if an SPV may be being used for fraud: What appears the reason for the SPV being used rather than another legal structure? Hiding ownership, etc. Does it fit the size and type of firm? Does it alter the risk of loss to the firm, or to my firm?

For regions where we do not have regulations around Fraud, what kind of minimum actions/controls should an organization follow?

The OCC Bulletin 2019-37 gives a really good overview of the sorts of high level best practices to be followed. Also, I say the following: measure fraud and monitor this over time and compared to peers, have multi-layer approach looking at authentication, limits, what's allowed in channels, along with fraud profiling, recovery actions, and education. Employees should also be monitored for fraud.

Meet the Experts



Ted Sausen
AML Subject Matter Expert NICE Actimize

Ted Sausen is a Subject Matter Expert within the NICE Actimize AML Line of Business. His role focuses on ensuring the Actimize AML technology solutions align with regulator expectations and the needs of the customer. Sausen has over 25 years of experience implementing global enterprise solutions across multiple industries including high tech, financial, transportation and manufacturing. He supported engineering, finance, supply chain, product safety and regulatory compliance. Prior to joining NICE Actimize, Mr. Sausen was a Senior Vice President at a large financial institution, leading the Global Compliance Analytics and Technology group. His role focused on implementing strategic solutions to fight financial crime, and supporting Global Economic Sanctions, AML Framework and Advisory, and the Financial Intelligence Unit. Sausen received his Certified Anti-Money Laundering Specialist (CAMS) Certification.



Rob Tharle
Fraud Subject Matter Expert NICE Actimize

Rob Tharle, Fraud & Authentication Subject Matter Expert, NICE Actimize EMEA, is responsible for providing thought leadership on industry trends, challenges and opportunities. Prior to joining NICE Actimize in 2019, he worked for 17 years in a number of Risk Management and Fraud Prevention roles at both Natwest/RBS and TSB. During that time, Tharle gained extensive experience with the technologies and design of fraud prevention and detection systems including application fraud, Apple and Google Pay, online and mobile banking.



NICE Actimize

Know more. Risk less

info@niceactimize.com
niceactimize.com/blog
@NICE_actimize
/company/actimize
NICEactimize

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

niceactimize.com