

Problem Shared.
Problem **Solved.**

The case for cooperation,
collaboration and communication
to fight financial crime



Silos: banking's silent menace

There's never been a better time to rob, compromise or break into a bank. Today, financial crime is vast in scale, bewildering in complexity and often committed remotely by criminals who face relatively low risk of being identified and prosecuted.

So, why is financial crime so rife right now? Just like any trend, there are many explanations. But one of the main reasons is that cyber criminals are able to exploit the internal silos and divisions within banks.

Criminals love silos

And the financial sector, currently weathering generational change, has more than a few. By their very nature, well-run banks and other financial institutions have enclaves and internal borders that ensure checks and balances, help enforce compliance and prevent fraudulent misbehavior or mishaps.

The inherently confidential nature of banking as well as the fact that banks compete commercially makes it hard to share knowledge and data (both internally and externally) on fraud, attacks or compromises.


Attackers can exploit this. They capitalize on divisions and borders within banks (and the wider financial sector) and turn an institution's defenses upon itself.


The good news

There are plenty of reasons to be concerned. But, equally, plenty of causes for optimism. The criminal threat can be addressed. It just requires us to think differently and adopt new approaches.

A more collaborative mindset within a financial institution can reap huge rewards for a relatively minor cost. Industry or sector-wide initiatives promise even greater benefits. To address the silo problem, banks should look to these types of common operating models, as well as open data sharing internally and externally, and industry-wide collaboration.

An example of one such opportunity is collaboration between the fraud and cyber security teams. Cyber teams have in-depth knowledge of the malware that targets customers. Fraud operations and strategy teams have a deep understanding of customer behaviors and how to identify fraudulent transactions. Given the very high proportion of fraud attacks which involve malware or some other cyber element, there are clear benefits to be had by banks who encourage these two teams to regularly share knowledge.





This paper can help **overhaul your bank's defenses** in a few months with minimal outlay. Internally sharing data, information and intelligence will **increase the effectiveness** of your compliance, fraud and cyber security teams.

Step by step

As this scenario shows, tackling silos is by no means farfetched conjecture. And even iterative, step-by-step improvements to internal lines of communication can return a tangible impact and bolster the human relationships that protect against financial crime.

What's more, the steps we're advocating are realistic, quick to implement and can deliver huge results – provided you adopt the right approach. This report guides you through that process.

More for less

This approach seeks to fight financial crime without a huge outlay, or a glacial roll-out spread over many years. It's not about trimming back or devoting fewer resources – time, employees, cash or management – to compliance, fraud and cyber security. Nor is it a raft of short-term sticking plasters. So, we're not proposing the merging of departments or buying the latest panacea.

What we advocate in this paper is promoting collaboration and communication to foster a pragmatic, insight-led and strategic approach to tackling financial crime. In doing so, intelligence can be shared, and potential avenues for criminals to exploit can be shut off – all without significant additional investment.

Breaking down silos, not hierarchies

It's worth noting that this approach is not about collapsing hierarchies or structures within a bank. We're recommending connecting different nodes, not destroying them.

Silos are often warranted – created to ensure that criminals or rogue employees can't get up to no good. In fact, individual silos can be a positive force, often nurturing and developing specialist knowledge. Experience and workflows would be effectively wiped out by removing internal borders altogether.



“The **key first step** is getting agreement between the compliance, fraud and cyber teams that a data problem exists.”

Start with the data

Data is both a huge opportunity and a huge headache. But no matter whether you’ve a glass half full or half empty perspective, there’s no denying that creating a new data storage and processing architecture is critical to the removal of silos.

The trouble is, the vast and varying data held by financial institutions is rarely ever uniform. The fields, thresholds and structures that one business unit looks for are often not the same as others. Combine this with multiple platforms and stores of diverse vintages, and simply managing the variety, volume and velocity of the data your organization processes is a significant task.

Then there are other more human considerations, like the cultural, legal and organizational issues around managing, accessing, modifying, storing and using data.

All of a sudden, finding a rigorous approach to data management and adopting a strong governance framework becomes extremely difficult.

Searching for answers

One seemingly obvious option might be to create a big data lake. The catch here is that it’s neither practical nor desirable to immediately build some sort of “brave new big data world”. With wildly different qualities, multiple datasets will quickly turn a new data lake into a data swamp. A more sophisticated and structured approach is needed.

Then there’s single detection engines and real-time analytics platforms. There’s no doubt they’re the future, but to properly harness their potential, data needs to be in the right place. Not always easy, especially if an organization has been through mergers and acquisitions. Plus, there’s the cost to consider.

Existing data warehouses might appear to be an easy answer from a non-technical manager’s perspective. Yet they’re built for batch processes, and there’s no room for real-time analysis. Great if you want to see what happened in detail a week or a day before, but not so wonderful if a new AML, fraud and cyber task force is looking to see what a single customer is doing right now.

Solving data silo dilemmas

Thankfully, there are short-term (and reassuringly practical) options. The key first step is getting agreement between the compliance, fraud and cyber teams that a data problem exists. And, subsequently, that data held in other silos can provide performance or efficiency improvements.

The next phase is to then hone in on the data itself. Specifically, that means taking the time to understand the lineage of each piece of data, and subsequently adopting a robust approach to data management – complemented by a sufficiently stable governance framework.

This dedication to understand the data is a crucial part of the equation – allowing an organization to rationalize and maximize the value of the data it holds. It goes almost without saying that an investment in capabilities to help exploit that data, and experiments to find hidden patterns of use and behavior, is a must. Business intelligence (BI) tools can be added into the mix, helping to simplify the reporting landscape and alleviate some of the burden IT staff will bear.

Five data silo challenges

1. **Real-time woes.** Siloed data warehouses are typically batch implementations. That means there's no room for real-time integration and exploitation, which is a critical requirement for fraud and cyber security.
2. **Finding a universal truth.** Often the lack of a common definition for a specific dataset is a barrier. It's difficult to know what data you hold if you can't agree how to categorize it.
3. **Handling multiple sources.** Banks are often simply not structured to serve business-specific use cases which require data from a number of sources. Fraud is a good example, where cyber security and compliance data can help to uncover fraud schemes.
4. **The legacy challenge.** Legacy systems remain a common stumbling block – a separate major task in and of themselves.
5. **Competing compliance requirements.** Compliance demands – not just financial but data management – are critical. On the one hand, it's important to manage data and privacy, as we've seen with GDPR. On the other, rapid access to data is key, especially with developments such as Open Banking.

“Sharing intelligence, information and data with the fraud strategy team allows a **mule account to be blacklisted or hotlisted.**”

#2



Tackle **specific** use cases

Few financial institutions are prepared to immediately make the leap to a common operating model for tackling crime. Instead, it's worth looking for small, measurable wins. Starting with the basics to prove the theory works can demonstrate the value while also allowing you to fine tune approaches and build alliances too.

Here's one short-term scenario – mule accounts. Compliance departments are often the first to spot these, but they are also highly relevant to other business units. Sharing intelligence, information and data with the fraud strategy team allows the account to be blacklisted or hotlisted. Then the cyber security team needs to be made aware – mule accounts are often the result of hacked or otherwise compromised accounts.

Other areas, such as payment fraud, may not call for an integrated approach in the short term. But while a bank's immediate focus is on aggregate transactions, longer term there'll still be a need for real-time fraud detection.

The value of staying specific

By focusing on explicit issues, challenges, or instances where silos pervade, you'll prove value, build momentum and encourage buy-in.

In the case of our example above, improving the flow of intelligence and information between internal departments when tackling mule accounts brings a number of benefits that'll attract business-wide support.

The first and most obvious is that once a compromised or fraudulent account is identified, it can be closed down. But this process may also provide intelligence that can lead to the identification of other suspect accounts, transactions and entities. For example, cyber and IT security teams often have specific information on attacks on banking networks or specific malware targeted against customers' machines. This critical insight can be invaluable to the fraud team.



Secondly, it empowers individual teams with the tools and knowhow to begin investigating the fringes of a suspicious, potentially fraudulent event. Fraud is nearly always cyber-enabled in some way or another. That's why regular updates from the cyber team are beneficial. Weekly notices and newsletters are a start, but banks can also enjoy significant benefits from monthly meetings between fraud and cyber teams.

Deeper dive – money mules

In most banks, the AML department is at the center of investigations into money mule accounts. This process sees criminals setting up operations using synthetic, real and compromised identities or accounts.

With some of the unnecessary barriers between fraud, compliance and cyber security removed, banks stand to benefit from simpler information sharing. The compliance department can distribute details of suspected mule accounts. This helps the fraud team to block or hotlist the accounts in their real-time fraud prevention program.

Compliance teams are also often involved in mule investigations. They can share their intelligence, data and information with third-party fraud teams to fill the gaps in a timeline that affects several bank departments. Not just cyber security and customer services, but the credit risk or credit abuse team too.

“With some of the **unnecessary barriers** between fraud, compliance and cyber security removed, banks stand to benefit from **simpler information sharing.**”

#3



“Challenger banks often have **fewer resources and people** devoted to fraud, if not cyber security and compliance.”

Involve **compliance, fraud and cyber** teams in new channel designs

The fast-paced nature of modern banking sees a continuous stream of new channels and services entering the market. That’s why it’s critical that security, fraud protection and compliance is built in at the beginning, not brought in at the end of a new product or channel’s development.

With more and more customers moving from in-branch interactions to phone, online and device-based app channels, the opportunities for criminals flourish. By ensuring fraud, compliance and cyber teams are involved from the inception of a channel, the internal teams setting up these new channels can help to identify possible risks and avenues of compromise early on.

Behavioral insights to dissuade potential wrongdoing can be powerful – and can prevent criminality before it begins, not after it has wreaked havoc.

For example, KYC (Know Your Customer) procedures built in to new channels can collect invaluable information, especially in peer to peer (P2P) channels. Moreover, the devices and identifying features in emerging channels (from originating phone numbers to IP addresses and device identities), can be used to uncover networks of compromised devices or identities.



Old and new

Many banking IT systems are often agglomerations, the result of M&A activity; typically big and cumbersome. Banks must therefore augment the information collected and employed by these old core systems with fresh data and systems. The silver lining to this cloud, however, is greater insight into customer behavior.

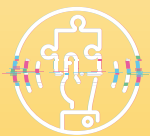
Meanwhile, challenger banks and smaller tier two operations do not necessarily have a competitive advantage resulting from a lack of legacy systems or their eager adoption of new channels. Challenger banks often have fewer resources and people devoted to fraud, if not cyber security and compliance.

Collaboration trumps isolation

These challenges are not necessarily something that can be or should be tackled in isolation. In particular, fraud is a community problem, and fraudulent transactions will often pass through more than just one bank before criminals cash out.

Both challenger and incumbent banks will benefit from involving fraud, cyber and compliance in new product design. However, it's vital to have a risk management process set up that considers the impact of new products and cyber, compliance and fraud risks collectively. This analysis then needs to turn into a plan for mitigation in both process and product design.

#4



“Building this **entity-centric approach** gives financial institutions a better understanding of customer behavior and a **better understanding of risk.**”

Adopt an **entity-centric** approach

Rather than looking at individual episodes of compromise, fraud and money laundering, there should be an effort to combine the insights, intelligence and data of all three teams to view patterns at the level of individual entities and groups of entities.

Building this entity-centric approach gives financial institutions a better understanding of customer behavior and a better understanding of risk. Some organizations will task their staff with investigating suspicious transactions. Others take an entity-centric view of alerts, and a network view of the problem.

By adopting the latter approach and plugging alerts into an entity's profile, banks can improve their understanding around the impact that certain activity may have and the risks that presents.

Risk score across lines of business

Similarly, another set of silos to break down are those between lines of business. A customer or entity may make large savings deposits, but also have a 'lively' current account set up and a suspicious range of loans and mortgages.

Building an encompassing risk score for an entity is a powerful business tool, but also means that high credit-risk customers can be monitored more closely by fraud and compliance teams.

It also boosts visibility. Removing silos allows for the swifter and simpler exiting of risky customers across all lines of an institution's business, as well as highlighting others that show subtle signs for concern.

For example, as a fraud team exits a customer from one line of business, they may realise that same person is a director of an organization that's a customer of another line of business, such as insurance or wealth management.

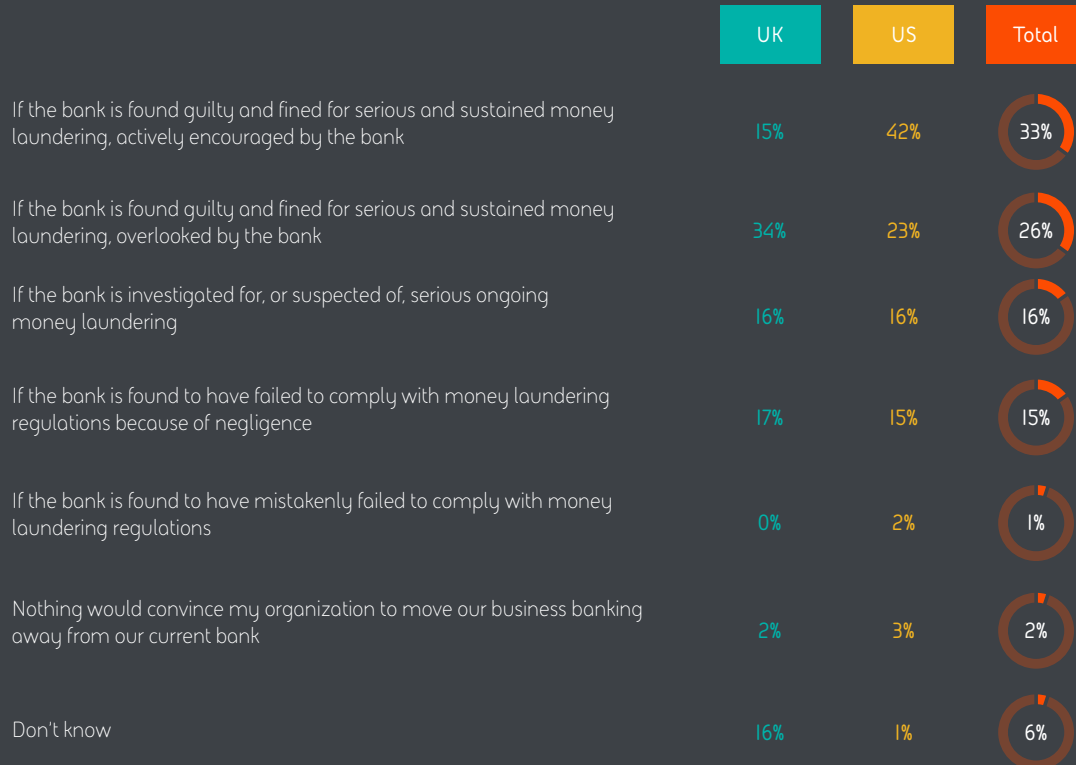
By adopting this entity-centric risk-scoring mantra, you'll benefit from greater visibility and a more comprehensive, intelligent fraud detection approach.

What would it take for you to move away from your current business bank?

In March 2018, we asked 300 technology professionals in the US and UK working at organizations with more than 1,000 employees about their attitudes to money laundering – and also what technology they thought banks used to defeat it.

Were our respondents willing to move their money to support the struggle? Despite the answers here, it's not clear that huge recent regulatory fines are sparking mass movements of customers.

Still, there appears to be a strong desire among customers for their banks to fight the good fight.



What do you think banks are doing to prevent money laundering?

Overall, technologists think Artificial Intelligence and Machine Learning are already used by banks to spot laundering – but that's not the case. In fact, AML solutions used by banks are often several years behind the curve and swamped with waves of false alerts. There's a concerted effort with the financial community to optimise existing solutions before pursuing advanced technology.

In the US, it's more about the high-tech solution, but in the UK, there's more focus on checks and policy:



Using machine learning and artificial intelligence to spot suspicious patterns

US: 74%

UK: 67%



Thorough background checks on anyone moving money in or out of their company

US: 63%

UK: 59%



Enforcing clear money laundering policies

US: 59%

UK: 58%



Relying on information from third parties

US: 37%

UK: 35%



Hiring lots of people to sort through large volumes of false alerts manually

US: 31%

UK: 23%



#5



Risk score across lines of business

Finally, teams need to work together to look for a standard detection engine that can serve the needs of all three units.

Despite fraud and compliance teams already looking for very similar signals and using similar data sets, consistency across all three parties is still extremely valuable. A common detection engine is important because it can be used to search and detect across multiple datasets, silos and stores.

To do this, teams need to compare notes and identify common formats, methodologies and sources. They're then in a position to standardize fields and set thresholds for alerts. The services of an enterprise architect can be useful at this juncture, to help build and put into production a virtualized data model.

“Teams need to compare notes and identify common formats, methodologies and sources. They're then in a position to **standardize fields and set thresholds** for alerts.”




“The next stage in the evolution of financial crime fighting centers **around increasing efficiency and getting better results** with the resources available.”

■ In conclusion

In recent years, financial institutions have thrown massive resources towards ensuring compliance and managing fraud risk. Despite this, they’ve still struggled to keep pace with the rapidly-evolving financial crime and fraud landscapes, and to respond to the growing impact of related cyber-crime.

The next stage in the evolution of financial crime fighting centers around increasing efficiency and getting better results with the resources available.

Many banks aspire to a single operating model with data fusion, enabled by machine learning, artificial intelligence and any other hyped technologies in the long term. But, as we’ve discussed, there are steps that can be taken here and now to break down silos. And, as a result, ways to increase effectiveness without creating huge disruption to your organization.



“By far the **most effective means** of doing this is improvement in internal lines of communication and cooperation.”

Focus on building the right culture

The most successful financial crime teams are focused primarily on the positive impacts for customers and wider society. In other words, first and foremost they want to do the right thing by driving criminals out of the bank. Compliance is often a secondary outcome. And a culture of collaboration is key here.


By far the most effective means of fighting financial crime is improving internal lines of communication and cooperation. Even seemingly small steps can generate noticeable improvements and help to establish the human relationships that make a united defense possible.




For more information on how to use cooperation, collaboration and communication to fight financial crime, visit baesystems.com/problemshared

BAE Systems, 1676 International Drive, Suite 1000, McLean, VA 22102, USA

E: learn@baesystems.com | W: baesystems.com/problemshared

 linkedin.com/company/baesystemsai

 twitter.com/baesystems_ai

Copyright © BAE Systems plc 2018. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.