



Building financial crime
resilience today to **future-proof**
banks for tomorrow



BAE SYSTEMS

■ Executive summary



Gareth Evans,
Senior Business
Solutions Consultant –
Fraud Prevention,
BAE Systems

The fast-evolving, sophisticated and increasingly global threat of financial crime is one of banking's biggest challenges. To be truly future-proof, institutions must move faster than the criminals who seek to attack them.

The financial sector is changing as never before. Open Banking, cryptocurrencies, artificial intelligence (AI), Big Data and cloud technologies are transforming the way people bank. Fintechs and challenger banks are widening the marketplace.

But those same advances bring opportunities for criminals as well – in terms of the types of crime committed, the perpetrators and their means of attack. They also render financial crime harder to identify and defeat.

One thing is clear. The most successful and profitable banks of tomorrow will be those that work hardest on financial crime prevention and defence today.

This paper explores some of the ways banking can future-proof itself against the growing financial crime challenge.



Financial crime-fighting costs dearly

The full extent of the challenge may be unclear, but that it constitutes a major expense for banks is not. The total annual bill for UK banks for combating cyber crime and online fraud is £6.7 billion, reports the Financial Conduct Authority¹ (FCA).

Banks prevented two-thirds of fraud attempts in 2018 (says UK Finance²), but in many cases a lack of support is making the job harder. One police force filed 96 per cent of well-evidenced fraud reports without further investigation, states a recent report from Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)³.

In America financial institutions are spending \$25.3 billion to meet their anti-money laundering compliance requirements,



£6.7bn

The total annual bill for UK banks for combating cyber crime and online fraud¹

¹ www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf


² <https://www.ukfinance.org.uk/press/press-releases/banking-industry-prevented-%C2%A3166-billion-fraud-2018>

³ www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf



\$25.3bn

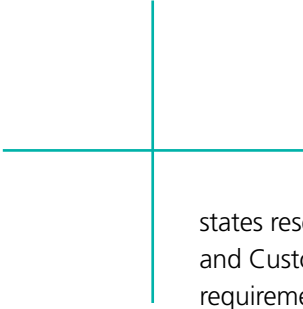
Annual cost to US financial institutions of AML compliance⁴



From 2010 to 2015 banks paid more than

£230bn

in fines related to non-compliance⁵



states research from LexisNexis⁴. For larger firms, this – plus Know Your Customer (KYC) and Customer Due Diligence (CDD) – brings the sum spent on meeting the regulatory requirement of fighting financial crime to more than £370 million in the UK.

Compliance is costly; as is non-compliance. From 2010 to 2015 banks paid more than £230 billion in fines related to non-compliance, says Accenture⁵. Future-proofing not only means fighting financial crime with real vigour, but also ensuring it is done in a way that is as time- and cost-efficient as possible.

Taking the lead

Those banks seizing the initiative look set to gain competitive advantage. And there are plenty of successful examples. The banks introducing the new ‘confirmation of payee’ service ahead of the 2020 regulatory deadline is just one.

Nordic banks are leading the way in the use of national digital identity schemes to fight fraud. Sweden’s BankID⁶ system has 75 per cent eligible population adoption. National Australia Bank meanwhile is developing biometric technology to protect customers from financial crime, working with Microsoft on biometric ATMs⁷. In the UK, £24.7 million of fraud has been prevented, says UK Finance⁸, thanks to the Banking Protocol⁹, a joint initiative between police and banks, aimed at identifying and protecting potential fraud victims.

⁴ <https://risk.lexisnexis.com/about-us/press-room/press-release/20181010-true-cost-aml>

⁵ <https://www.accenture.com/gb-en/insights/artificial-intelligence/intelligent-financial-crime-detection>

⁶ www.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx

⁷ www.biometricupdate.com/201810/nab-and-microsoft-collaborate-on-biometric-atm-concept

⁸ www.ukfinance.org.uk/press/press-releases/banking-industry-prevented-£166-billion-fraud-2018

⁹ <https://www.ukfinance.org.uk/news-and-insight/blogs/why-banking-protocol-matters>





A changing landscape: Open Banking

The global shift towards Open Banking is revolutionising financial services. The Second Payment Services Directive (PSD2) – final compliance deadline September 2019 – is not only a business opportunity for banks, but also a new security challenge. This legislation may apply only to the European Economic Area, but its principles are being mirrored elsewhere.

Gareth Evans, senior business solutions consultant at BAE Systems Applied Intelligence, is clear about the benefits: “There are opportunities for somebody to be an account service provider bringing all of a customer’s balances into one place, enabling them to keep a single view of their finances and offering reports on how to get better deals or improve credit.”

Open Banking aims to break the cartel of big banks and open the industry to competition. It is currently unclear where responsibility for security vulnerabilities accompanying these changes will lie and banks must step up security in preparation.

“Banks used to be a building with one big, heavy door to keep an eye on. If you stole from the bank you had to kick the door down”

Gareth Evans

At present, mobile payment systems operate as mobile wallets, with a card for payment. Evans thinks Open Banking will eventually allow them to debit money directly, saving on transaction fees. The security implications are clear.

“Banks used to be a building with one big, heavy door to keep an eye on,” says Evans. “If you stole from the bank you had to kick the door down. Cheques, cards and mobile internet banking have effectively added more doors. And the doors aren’t always controlled by the banks, so security is reliant on different parties.”

At the same time banks face increased pressure to accept more liability for customer fraud losses. In the UK, the Authorised Push Payment (APP) Scams Steering Group, established by the Payment Systems Regulator, has developed a voluntary code for reimbursing victims introduced in May 2019¹⁰.

Closing the doors on crime

So how can banks ensure Open Banking does not leave them vulnerable to attack; opening new doors to customers, but not to criminals?

¹⁰ <https://appcrmsteeringgroup.uk/wp-content/uploads/2019/02/APP-scams-Steering-Group-Final-CRM-Code.pdf>

“No matter how good the lock on your door, sooner or later someone will break in. When they do, how do you monitor them?”

Gareth Evans

One approach, says Evans, is to sharpen targeted monitoring used to assess transaction risk. “Typically they look at who’s making the transaction, the way they are they doing it, the method and where the transaction is going.”

This is no longer enough. “The transaction is now coming from a third party. Banks need to be able to interpret new information. They must evolve their detection capabilities to use it.”

Lessons for Europe can be found elsewhere. The Monetary Authority of Singapore and the country’s Association of Banks have published an API Playbook¹¹ to support data exchange and communication between banks and fintechs. Japanese banks, meanwhile, are required to publish their open API policies and encouraged to contract with a single third-party provider by 2020.

Detection and protection in Open Banking

Financial institutions are already obliged to meet certain standards in authentication to operate Open Banking, of course.

Banks typically operate two types of detection: covert and overt. Overt protections – authentication tools and biometrics – add hurdles for the criminal and reassure the customer. Covert technologies enable banks to see what’s happening once a criminal gets into an account. This, says Evans, will be increasingly important. “No matter how good the lock on your door, sooner or later someone will break in. When they do, how do you monitor them?”

If banks are to be future-proof, they must work on covert model risk tool analytics to understand this new landscape with its varying risks. A customer arriving from an authorised banking app is likely to inspire more confidence than one from an unknown source, for instance.

¹¹ <http://www.mas.gov.sg/~media/Smart%20Financial%20Centre/API/ABSMASAPIPlaybook.pdf>



Future-proofing payments: the cryptocurrency criminal

Cryptocurrencies operating outside of central banks pose new risks. The Bank of England's Financial Policy Committee recognises the benefits of these currencies and their potential to create a more distributed and diverse payments system. However, it also warns that they are unpredictable and unprotected.

Numerous authorities, including the UK Cryptoassets Taskforce – which comprises the FCA, Bank of England and HM Treasury – are urging crypto-focused regulation.

“Most people thought cryptocurrency would peak and disappear,” says Evans, with the result that not enough attention has been paid to robust protections. Instead the technologies have grown, with an attendant rise in related fraud.

In June and July 2018 alone, victims reported losing £2,059,501 to cryptocurrency scams, figures from Action Fraud¹² show. “A lot of unscrupulous people made a lot of money creating their own cryptocurrencies and taking money from trusting people who invested and have never had a return,” he says.

Evans predicts crypto technology and bank accounts will converge. JP Morgan Chase has already announced plans¹³ to launch a cryptocurrency, the first to be backed by a large US bank.

“Perhaps through Open Banking someone will create a product allowing customers to take money from a bank account, transfer it through cryptocurrency and then turn it back into cash again,” says Evans.

Such swapping between cash and cryptocurrency is an attractive proposition for fraudsters. “Right now, a criminal can get into a bank account, send the money to another account that they can control, take the money out as cash and convert it into Bitcoin,” says Evans. “Our systems trace that money.”

¹² www.actionfraud.police.uk/alert/2m-lost-to-cryptocurrency-fraud

¹³ <https://www.jpmorgan.com/global/news/digital-coin-payments>



Money laundering and cryptocurrency: shifting liability

Money laundering enables serious and organised crime, costing the UK £24 billion a year says the National Crime Agency¹⁴. With their links to terrorist financing and people trafficking, it is right that the spotlight is now on the role of cryptocurrencies in the trail of dirty money.

Financial institutions currently take the hit for cryptocurrency-enabled financial crime. This, Evans insists, is a live issue. "Sooner or later the authorities are going to have to look at how Bitcoin is being used," he says. "Are the exchanges going to find themselves liable for money laundering checks?" The argument that they are simply a gateway, free from responsibility, may prove unsustainable.

One outcome, he suggests, could be the swapping of roles between banks and exchanges. "The exchanges might become the banks. Or the exchanges might be shut down because of money laundering and therefore the banks become the exchanges. This leaves the banks holding the money-laundering risk."

As liability changes, so too will the financial landscape. Its new shape is not yet clear, but banks must nevertheless prepare for change. The financial, reputational and societal costs involved are high.

¹⁴ <https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing>





Tomorrow's technology: the AI revolution

AI holds huge potential for banks, not only in the fight to retain customers, but also as a weapon against financial crime.

Chris Gibson, former director of CERT-UK, the UK national computer emergency response team, says AI will be vital in the challenging landscape of faster and ever growing numbers of global transactions. "AI will hopefully allow us to crunch through the vast data stores we're creating to find the needle in the haystack," he says. "We need smarter and better ways to perform analysis."

Technology allows banks to gather increasingly accurate information about customers' wants and behaviours. Transactions in line with earlier behaviours will go unchallenged. But those involving, for example, the transfer of an unusually large sum or one to an unknown party can trigger an alert. It also helps banks build fraud profiles and track criminals through financial networks.

Even more valuable in future will be AI's ability to identify groups of tiny potentially fraudulent transactions – sums that would individually fly below the radar of even highly trained fraud experts, but could collectively add up to huge sums. Banks may also use AI to review extra data, such as customers' social media and work history, to determine whether actions are in line with demographic expectations.

With much financial crime assisted by corrupt insiders, AI promises further advantages – as Adam Williamson¹⁵, head of professional standards at the UK's Association of Accounting Technicians (AAT) recently told the BBC. "Using AI removes much of the risk of people deliberately overlooking suspicious activity," he said.

¹⁵ <https://www.bbc.co.uk/news/business-47772362>



With AI, banks will be able to
respond better and crucially
quicker to cyber crime

"AI needs to serve a business process and it requires input from across an institution, not just from technology"

Chris Gibson

For the majority of trustworthy bank employees, AI will free time previously spent on mundane vigilance and the investigation of false positives in favour of work on crime prevention and detection. Those banks employing AI to best effect will find error detection, productivity and decision-making improved.

But banks have work to do if AI is to live up to its future-proofing potential. The technology needs data – and there isn't yet enough of it. The solution must, in part, involve the effective sharing of resources across the industry. In January, the Economic Crime Strategic Board was established in the UK, with data sharing as a priority.

Within companies, too, collaboration on the collation and use of data is crucial. "AI needs to serve a business process and, as such, it requires input from across an institution, not just from technology," says Chris Gibson.

With AI, banks will be able to respond better and crucially quicker to cyber crime. A shortage of cyber professionals to do such work in person means this is vital in the battle to beat financial crime.

Mariola Marzouk, BAE Systems' global head of financial crime and fraud insights, says ensuring that human expertise is most efficiently deployed is crucial in future-proofing. "Collecting data is where investigators spend 60 per cent of their time," she says. With AI, banks can better combine their CRM data gathered from a customer or an external source with behavioural data in the form of transactions. "This way we can tell if a customer behaves the way they told us they would – and if not, why they might have changed and what this means from a crime perspective."

AI and the criminal

Artificial intelligence comes with a major caveat. Banks must look at who else is using the technology. If financial institutions see its benefits, so too will criminals. Chris Gibson says: "I'm constantly surprised that the criminals aren't, or don't appear to be, using AI all that much.

"Everything we know about them tells us they are very focused and business minded. This must be an area that would enhance their profit margins."

AI then can offer solutions. Clearly it must be part of the industry's toolkit in the battle against fraud, but it must be employed correctly. Financial institutions must first grasp the problem they want it to solve, in detail. They need to work together to understand the data they are using – both its provenance and its context. They need to know its attendant risks. And they need to be ready for the criminals to be using it, too.

Challenges for challengers

New entrants are changing banking. This is a busy marketplace. But newcomers and established banks should look to each other for lessons in future-proofing.

While smaller fintech companies and newer banks might offer a fast and frictionless experience – highly appealing to modern consumers – this can come at the price of proper customer onboarding, causing problems later.

Mariola Marzouk highlights the case of a UK fintech that was originally a prepaid card provider. The company offered a very good interest rate, especially attractive to international travellers, with little customer verification.

“The process of collecting information is probably the most **time-consuming** thing for banks and it’s also very customer-sensitive”

Mariola Marzouk

Problems arose, however, when it wanted to increase the prepaid card amount. Regulation changed and the company found itself with time-consuming and costly due diligence obligations. This, says Marzouk, is where challengers start to experience the same problems as larger banks. “The process of collecting information is probably the most time-consuming thing for banks and it’s also very customer-sensitive.”

In contrast to the challengers’ problems, Marzouk describes the bold approach to compliance taken by one big UK bank. Large numbers of regulators have been hired to help with compliance, alongside a former investigator to lead its crime division. Now, when a customer onboards at the bank, they are assigned a risk score according to their likelihood of committing financial crime. “You will be judged from the minute you’re onboarded,” says Marzouk. “They will monitor your behaviour and whether you might be more likely to be more complacent or to eventually commit a crime, and they will do this non-stop.”

Finding the balance

There is a balance to be struck, says Marzouk. Doing so will be key to winning competitive advantage. Security cannot be side-stepped and it must be ongoing, but banks should tread carefully. “They need to pay close attention to making sure they do not upset legitimate customers or make them feel like they are criminals.”

As challengers grow and find themselves bound by more regulation, they risk becoming less attractive to customers. Here they can learn from the KYC and onboarding processes of larger organisations, hiring regulatory specialists to work for them.



The real challenge for banks is not only to work out the technologies enabling crime today, but also those that will do so tomorrow

Equally, challengers can offer valuable future-proofing lessons to their longer established competitors. The former's younger infrastructure and greater agility, with digital customer verification in-built early on, means they often manage threats better.

The correct approach to regulation will help maximise advantage – as well as ensure the benefits of its intended financial crime prevention. There is a utility curve, says Marzouk. "At one point, regulations are good because people won't do things they shouldn't. But then it gets to the level where it's too much, the regulations become onerous and you have to spend more to comply."

Here again, industry-wide collaboration will be needed to ensure the right level of regulation in the face of the criminal threat. Fraudsters, of course, are finding their own solutions to these defences, says Marzouk. "They are responding to these increased regulations, spending more on circumventing regulation, engaging professional enablers and corrupt law enforcers, which in turn makes it even more difficult to detect fraud."

One tactic employed by criminals has been the use of trusts. Confidentiality agreements around these financial products make it harder to identify the owner. The vast majority are established with legitimate aims, but the mechanism for differentiation is lacking.


The combination of legitimate business with illegal business to 'hide the noise' is another area where appropriate regulation could help illuminate the shadowy corners.

The real challenge for banks is not only to work out the technologies enabling crime today, but also those that will do so tomorrow. Marzouk says: "We are fixating on how criminals might be using digital currencies, for instance. But they are probably also using something we don't even know about yet."



Future-proofing wins customers and keeps them

Preventing and detecting financial crime is crucial to building a future-proof bank, but so is ensuring the best response when it does happen. Banks can build competitive advantage by their approach to crime detection and the ways in which they deal with the aftermath of a breach or attack.



Alex Jay, dispute resolution partner at multinational law firm, Gowling WLG and a member of the Fraud Advisory Panel, believes customer satisfaction is an important driver in financial crime prevention. “Banks will invest huge amounts of money and time in systems that try to identify and prevent fraud because they know that if they are dealing with customers who have suffered a fraud, which is in broad terms not their fault, the bank ends up picking up the tab. And they want to look after their customers, too.”

Effective use of AI, he believes, as well as ongoing vigilance, must be priorities for banking because it operates in an increasingly global sphere.

Only the most scrupulous KYC processes and the best technology – applied throughout a company – will allow banks to successfully navigate the changing financial landscape, promptly and accurately differentiating the fraudulent activity from the legitimate.

■ Conclusion

Financial crime is not going away and is, if anything, growing. Companies are now losing an average of 7 per cent of annual expenditure to fraud, with the global cost now topping £3 trillion, finds research from Crowe Clark Whitehill¹⁶.

Technology is fanning the flames of a criminal impulse which has existed as long as banking itself. Jamie Dimon, JPMorgan Chase Chairman and CEO recently deemed cyber concerns “probably the biggest risk the financial system faces”¹⁷. In the UK, 54 per cent of 2018 fraud cases were cyber-related, according to government¹⁸ figures.

Developing robust, rapid and effective systems to prevent financial crime and deal with the fallout will matter even more tomorrow than today. As criminals devise increasingly sophisticated systems to identify and bypass security measures, banks must stay ahead.

The obligation is not just a financial, but a social one. “We all have a social duty to prevent crime, whatever size the organisation. Humanity cannot grow if it doesn’t share information, knowledge and experience,” says Marzouk.

In 1994, Bill Gates¹⁹ famously decreed banks to be ‘dinosaurs’, saying they could be bypassed. If extinction seems unlikely, evolution is certainly necessary. The form of banking in the future will depend, in part, on how well the industry works to fight the threats on the horizon. The battle has begun.

¹⁶ <https://www.accountancydaily.co/global-cost-fraud-tops-ps3-trillion>

¹⁷ <https://bankingjournal.aba.com/2019/04/large-bank-ceos-raise-concerns-about-cybersecurity-slowing-global-growth/>

¹⁸ <https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/51507.htm>

¹⁹ <https://25iq.com/quotations/bill-gates/>

■ What next?

Banks that future-proof their compliance and fraud teams will represent a harder target to criminal enterprises. But there is also a strong argument for active and early co-operation with competitors, regulators and law enforcement, rather than merely responding to criminal threats.

Internal change

Open Banking is a big opportunity for established institutions, startups and adjacent industries to address crime and reset customer expectations of what their bank should do for them. Engagement with internal innovation teams, external organisations and partners is vital. Core to this is close co-operation between cyber security, fraud and compliance functions.

Building holistic entity and customer views

An accurate view of your customers – and what risks they represent – is vital. Holistic views are not only a powerful compliance and counter fraud tool, but also an opportunity to upsell and cross-sell to existing customers – an important consideration in a market where a retail customer can cost up to \$2,000 to acquire.

Building the perfect human/machine partnerships

We help banks hand the repetitive work to the robots and automate as much of the process as possible to free up human employees, boosting effectiveness across the board. Machine learning, artificial intelligence and robotic process automation have much to bring to the table. Successful organisations combine human and machine intelligence.

For more information go to:
www.boesystems.com/bankinginsights

Contact us

E: learn@baesystems.com

W: baesystems.com/bankinginsights

**Victim of a cyber attack? Contact our
emergency response team on:**

US: 1 (800) 417-2155

UK: 0808 168 6647

Australia: 1800 825 411

International: +44 1483 817491

E: cyberresponse@baesystems.com

Copyright © BAE Systems plc 2019. 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.



linkedin.com/company/baesystemsai



twitter.com/baesystems_ai