LexisNexis®
RISK SOLUTIONS

ON THE FRONTLINE

FINTECHS VS MONEY LAUNDERING

MONEY LAUNDERING
EXPOSED

Written by The Economist INTELLIGENCE UNIT

FOREWORD

When it comes to financial technology (fintech) the UK is a global leader. Investment in the fintech sector continues to grow, reflecting the strong belief investors have in the UK financial services sector's ability to innovate, be efficient and remain globally competitive.

However, the UK is also a global hub for money laundering and other types of financial crime. So just how well is the sector embracing the need to build systems, which also tackle the growing twin challenges of greater financial regulation and growing fraud and money laundering?

This article aims to discover how the fintech sector, including challenger banks, digital payment processors and card service providers, thinks it is doing in the fight against financial crime. It also investigates what the financial crime challenges mean for the sector.

Fintechs, by their very nature, are not encumbered by legacy systems. They are generally more streamlined and less complex in terms of their operations, products and services and therefore should be able to quickly implement cutting edge solutions to combat growing fraud and money laundering. The question that this article explores is whether it has the motivation and aptitude to do so.

Still, the fintechs do share two of the same limitations as more established financial service providers: access to people with expertise in financial crime compliance and high quality data. Both of these factors are crucial in being able to identify new and emerging financial crime methodologies.

Our thanks to the Economist Intelligence Unit who conducted the interviews and reported the findings on behalf of LexisNexis® Risk Solutions.

We sincerely hope you find this research both interesting and useful. LexisNexis Risk Solutions is also part of the fintech community and continues to invest heavily in both technology and data, along with the many firms interviewed for this report.

"IT IS ABOUT WHAT DATA YOU COLLECT PER TRANSACTION AND CUSTOMER, NOT JUST HOW MUCH TRANSACTION DATA YOU COLLECT."

KEY FINDINGS

- According to a survey conducted by The Economist Intelligence Unit on behalf of LexisNexis® Risk Solutions, financial technology firms (fintechs) are the most sceptical that the UK's anti-money laundering (AML) regime is fit for purpose. Twelve percent of fintechs believe the collective effort is insufficient, compared with 9% across other regulated sectors.
- They are more likely to see corporate and investment banks (ranked the sector most at risk by 15%, reaching 20% for larger fintechs) and gaming firms (20%) as the weak links, rather than real-estate agents (5%), accountants (3%) or tax advisers (2%).
- The Proceeds of Crime Act (POCA) and the Suspicious Activity Report (SAR) regime hamper fintechs from being more proactive in sharing their digital footprint data for the good of all.
- Data sharing will require all regulated businesses and enforcement agencies to contribute and act consistently, aided by clearer regulatory guidance.

Challenger banks and new fintech payment initiators are well placed to be successful in fighting money laundering. They have three advantages over many traditional banks: they operate new systems; their product ranges and corporate structures are simple; and, most importantly, according to our survey, they display a willingness to work with others in the collective battle against criminals.

BLANK SLATE

Fintech newcomers are without the baggage carried by traditional banks. They do not have to spend millions on keeping legacy systems running and they tend to have a single integrated architecture. This allows them to place AML procedures at the heart of their operations, not layer it on a complex web of pre-existing systems.

New service providers, whether challenger banks or card issuers, also have a slimmer product range, making money and unusual behaviour easier to track through their systems. App and mobile-based services can access a wealth of information on their customers that goes further than traditional Know Your Customer and transaction data ever could.

As an app-only business, challenger bank Monzo is able to collect a much wider set of data than its traditional counterparts operating through retail branches and online banking, explains Natasha Vernier, head of financial crime at Monzo. "It is about what data you collect per transaction and customer, not just how much transaction data you collect," she says.

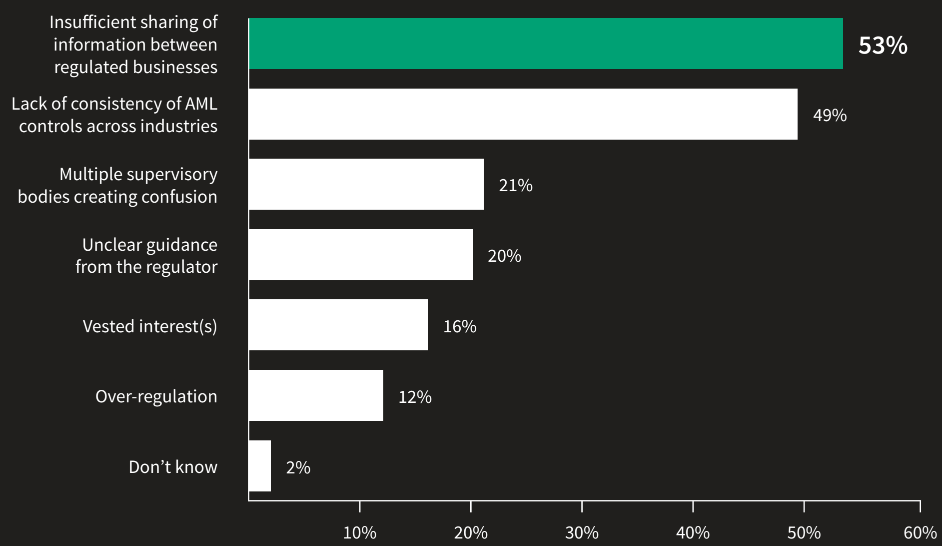
COMPLEXITY AND CONSISTENCY

Nearly one in eight fintechs (12%) say the collective effort to tackle money laundering is not good enough, compared with 9% across all sectors surveyed. Almost four in ten fintech respondents (39%) cite corporate and investment banks in the three sectors they consider most at risk, far more than traditional banks do themselves (28%).

For Ms Vernier, the explanation is simple: traditional banks are complex, with multiple product lines, distribution channels, business units and systems. Customers may see a unified brand, while in fact internal processes and departments may struggle to communicate efficiently.

E-payment providers and new banking app firms have lower barriers to entry, notably by way of capital requirements, but they must comply fully with all AML regulatory requirements. Few feel like they should be offered special terms. In fact, smaller fintechs are more likely to say that the current regulation is proportionate to the money laundering threat they face (58%) than their larger peers (47%).

Figure 1
Biggest external barriers to efficient AML (n=61)



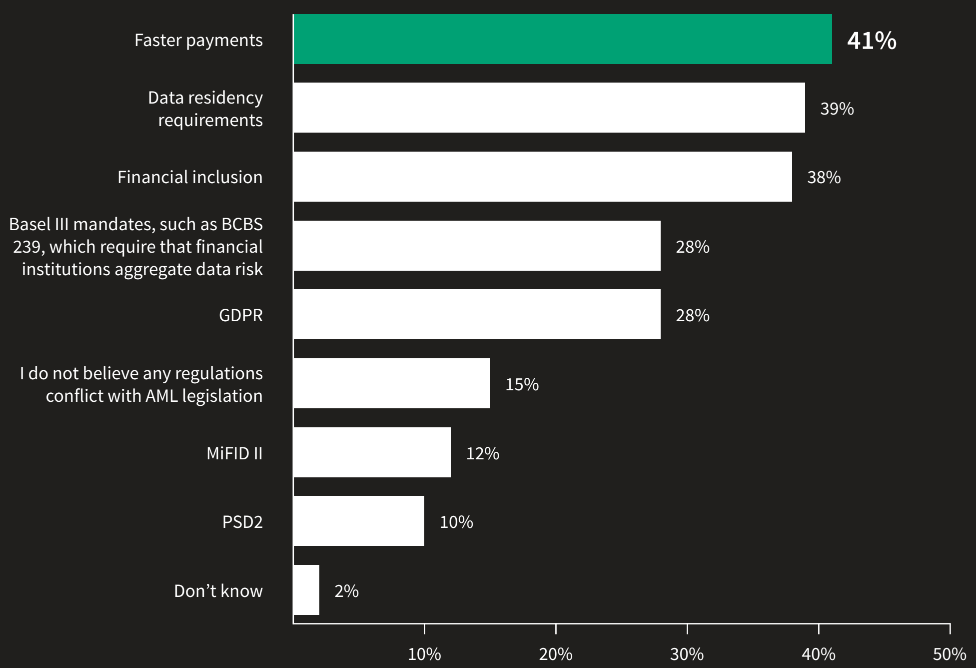
Regardless of size, regulatory demands (12%) are low on their list of complaints: how those rules are put into practice counts for more. When asked about the biggest external barriers to efficient AML, around half of fintech respondents cited a lack of consistency across regulated sectors (49%) and insufficient data sharing (53%). This suggests a stronger desire for collaboration than felt by traditional banks and other regulated sectors, which both cited insufficient data sharing at 43%.

POLICY MATTERS

In an industry reliant on speed, data and convenience, it comes as no surprise that Faster Payments (41%) and data residency (39%) sit high on the fintech list of regulations conflicting with AML legislation.

The Open Banking initiative, under the revised EU Payment Services Directive (PSD2), is perceived as less of a source of conflict with AML regulation than other regulations (10%). The initiative forces banks to share information with competitors through common application programming interfaces. These may open up certain risks, particularly around cyber-security, yet many in the industry see the software protocols as a positive tool in the fight against money laundering.

Figure 2
Regulations conflicting with AML (n=61)



"You could send a Faster Payment with a risk weighting. The receiving bank would then pay a little more attention to how the customer uses the money," Ms Vernier says.

This would allow suspicious flows to be tracked by the National Crime Agency (NCA) and, if necessary, frozen. If innocent customers are defrauded in the process, their funds could also be returned far quicker, she explains.

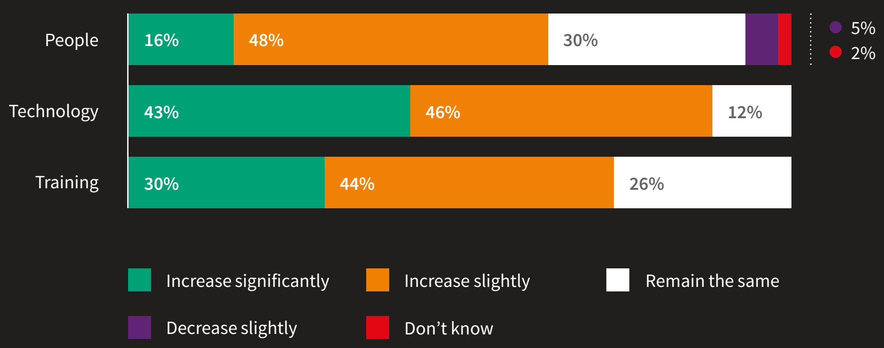
Moreover, Ms Vernier believes banks could harmonise the way they send information about suspicious payments. For instance, Monzo receives many notifications of flagged transactions by email. Some are encrypted and others are linked to secure websites, making it hard for Monzo, as a recipient bank, to automate its follow-up processes.

FINTECHS HAVE NO CHOICE BUT TO INVEST HEAVILY IN AML STAFF AND SYSTEMS.

TECHNOLOGY AND CULTURE

Fintechs have no choice but to invest heavily in AML staff and systems. People and training take up almost two-thirds of their budget, an amount in line with other regulated businesses. Recruiting employees with the right skill set can be an issue, as they are also competing against incumbents who have far bigger budgets. Indeed, 46% of banks have a greater than £1m AML compliance budget to work with, compared with 33% of fintechs. Banks are also more likely to see their budget for staff (70%) and training (82%) increase over the next 3-5 years than their challenger counterparts (64% and 74% for people and training, respectively).

Figure 3
Evolution of AML costs over next 3-5 years (n=61)



As would be expected, almost half (46%) of fintechs, a figure that reaches 60% for those with revenue above £500m, view new technologies such as artificial intelligence and advanced analytics as one of the most efficient ways to improve the fight against money laundering.

This keenness for cutting-edge technologies may be the reason why fintechs are twice as likely (8%) as other respondents (4%) to say their AML compliance costs have risen by more than 30% over the past 24 months, although staff costs (predicted by 16% to increase significantly) could fall back in line with other sectors, where a steep hike is expected by 23%.

That said, the bigger concern might not be resources (25%), but corporate culture. Fintechs are more likely than other respondent groups to cite complacency (43%) and a lack of understanding of money laundering methodologies (48%) as the biggest internal barriers to fighting money laundering.

Nearly four in ten (38%) fintechs want company cultures to change from apathy, or one of simply box ticking to avoid fines, to one that actively halts money laundering in its tracks. Training to a high standard would help, with more than a third (34%) of respondents believing that corporate effectiveness will be improved if all staff received the same education on financial crime risk as senior managers and compliance professionals do.

“We want to do one thing really well, which allows us to have a consistent understanding across our entire team of what we are offering and what the risks of that product are, and a consistent mitigating approach. More and more businesses are trying to do the same thing,” says Ben Steyn, head of compliance and money laundering reporting officer at Transferwise.

BETTER FEEDBACK AND PROACTIVITY FROM ENFORCEMENT AGENCIES COULD ENCOURAGE FINTECHS TO DO MORE.

INFORMATION SHARING

Likewise, as criminals become more sophisticated, intermediaries need an incentive to keep improving their AML processes. While regulation often lags real life, better feedback and proactivity from enforcement agencies could be a way to encourage fintechs to do more. Conveying the actual outcomes of SARs back to the companies that wrote them would be a good start (18%).

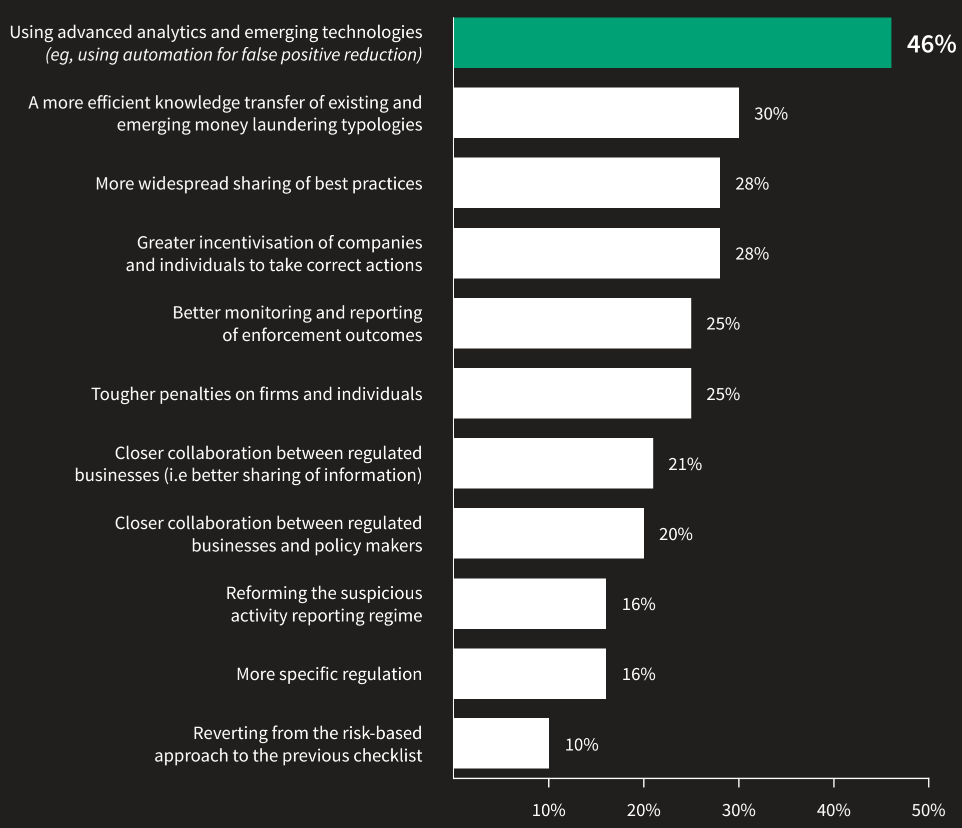
Under the UK's "all crimes" approach, the POCA requires all regulated firms to file SARs to the NCA. But, in practice, the NCA is not a general crime-reporting agency; its strategy and resources are focused on big, material cases, not individual low-value transactions.

"We are often stuck between a rock and a hard place, where we need to be able to satisfy the regulation, yet for a £20 or £100 transaction, the NCA won't spend much time looking at those. But if we don't, we fall foul of the regulation," says Mr Steyn.

More than half of fintech respondents (54%) believe a better use of technology will improve the SAR process, as will more information sharing (44%).

In fact, when considering the best ways to improve AML altogether, besides using advanced technologies (46%), fintechs are eager to share what they learn from their AML processes. They believe they can help others work better by pooling experience and information on the new schemes criminals are using to launder money (30%), but also want measures to encourage personal and corporate responsibility to stamp out money laundering (28%).

Figure 4
Most effective ways to improve AML (n=61)



What are most missing at present, Mr Steyn thinks, are the ability to share data effectively with the NCA for enforcement action and, perhaps more importantly, easier ways to share the knowledge for the good of the financial industry and regulated sectors as a whole.

WE CANNOT BE COMPLACENT

APPENDIX

THE SURVEY

The survey was conducted by The Economist Intelligence Unit on behalf of LexisNexis® Risk Solutions from December 2018 to March 2019. More than 200 senior compliance, finance and legal executives from regulated sectors (banking and financial services, legal, real estate and gaming) participated in the survey. The survey asked respondents about their views on risk, government policy, regulation, internal procedures and technology. The survey sought to examine the most effective measures to be deployed to ensure that private sector and enforcement agencies can spot criminals and illicit flows of money in, around and out of the UK.

This article is based on the views of 61 participants from the fintech industry, all of which are responsible for AML compliance. This included 31 respondents from fintechs with revenue under £500m, and 30 respondents from larger fintechs (revenue over £500m).

We are grateful to the following for sharing their insights and real-life experiences:

- Ben Steyn, head of compliance, Transferwise
- Natasha Vernier, head of financial crime, Monzo

REMEMBER WHAT
WE’RE FIGHTING FOR

For more information, call 029 2067 8555
or email ukenquiry@lexisnexis.com

risk.lexisnexis.co.uk

LexisNexis®
RISK SOLUTIONS

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers across industries. For more information, please visit risk.lexisnexis.co.uk and www.relx.com.