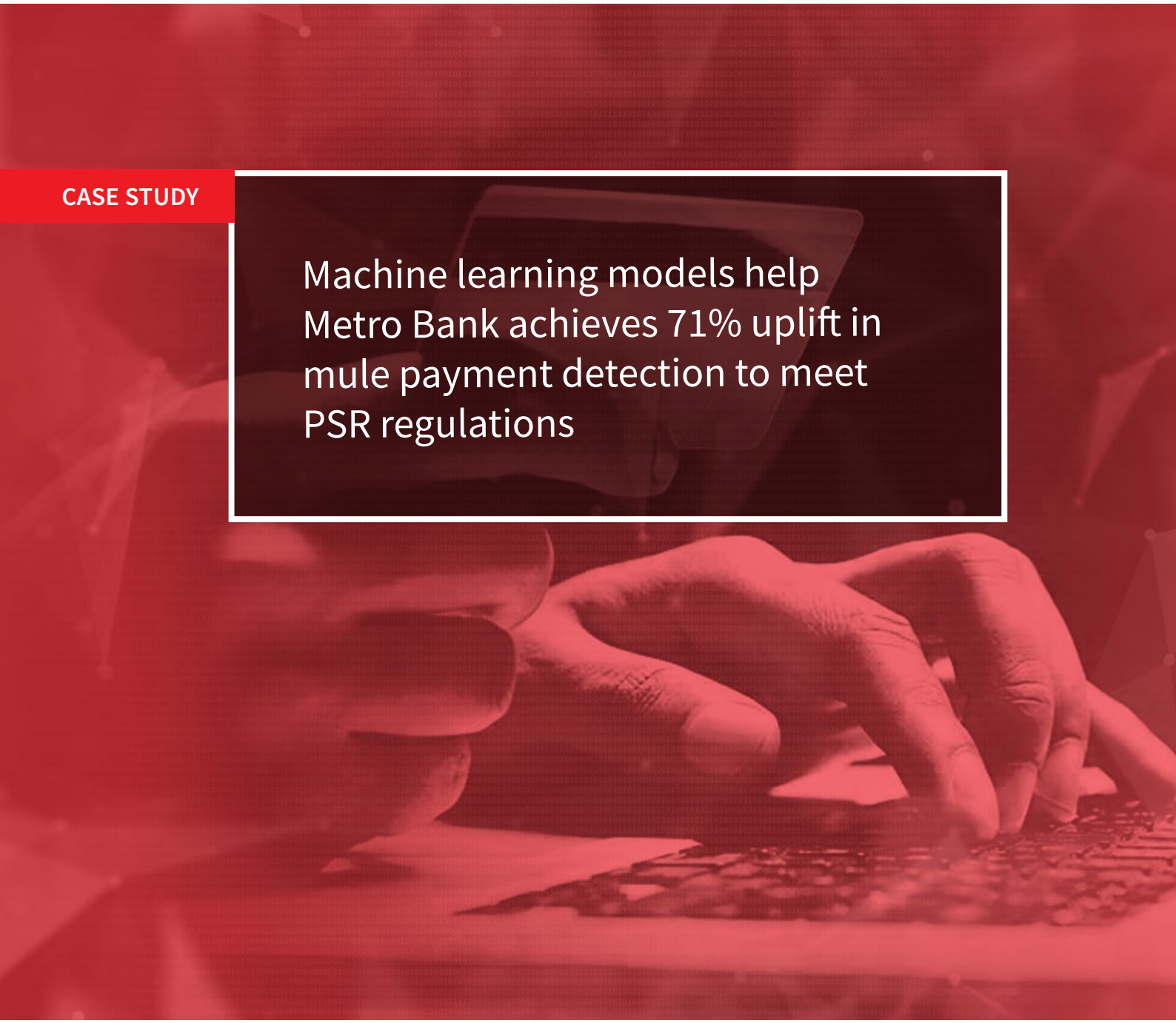
LexisNexis® RISK SOLUTIONS

METRO BANK

CASE STUDY

Machine learning models help Metro Bank achieves 71% uplift in mule payment detection to meet PSR regulations



Captured mule payments could have cost the bank around £5 million in victim reimbursement costs annually, under new PSR rules

A race against time

The Payment Systems Regulator (PSR) rules on statutory customer reimbursement of authorised push payment (APP) scam losses brought about significant changes to the UK banking sector. The reforms, implemented in October 2024, placed a 50:50 liability on both the victim's bank and the recipient financial institution. UK banks needed to configure processes to mitigate the risk of unwittingly onboarding fraudulent customers or allowing fraudulent funds to be received into customer accounts. Failure to do either could potentially lead to significant increases in reimbursements to scam victims, with an inevitable impact on operating profits. Metro Bank teamed up with LexisNexis® Risk Solutions to tackle the PSR challenge head-on, yielding some impressive results.

Challenges to identify money mules

All payment fraud shares common characteristics, a key one being that a beneficiary account is always required, in order to receive the victim's money. Once acquired, the funds may be laundered across a network of other mule accounts, with each movement of funds increasing the difficulty for law enforcement to track the predicate activity. In just a few minutes, the money can all but disappear, leaving the fraudsters free to reap the profits. To make matters worse, money mules can operate in a variety of ways, posing a challenge to financial institutions in identifying what exactly constitutes suspicious behaviour.

Complicit mule accounts – i.e. those explicitly set up to knowingly receive fraudulent funds. Typically, they begin their illicit activity shortly after creation. Once the account is open, the mule may try to move funds as quickly as possible to avoid detection, using a series of transfers under their control. In other cases, accounts may be dormant for an extended period after opening, before seeing a sudden spike in low-value payments, designed to build a legitimate payment history, followed by the movement of laundered funds in their control.

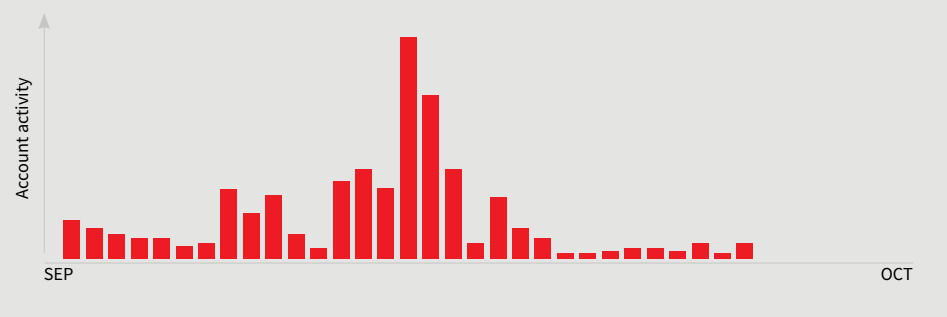


Fig.1: *Above is a visual representation of a mule's activity in the LexisNexis® ThreatMetrix® portal. Shortly after opening the account, we see a high volume of mule login and payment activity. During this period, the mule is frequently checking their account to confirm receipt of funds before making outbound payments to other mule accounts. Once the activity is complete, the account is no longer in use.*

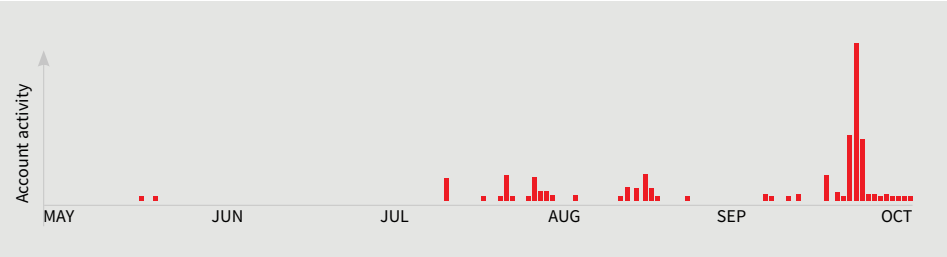
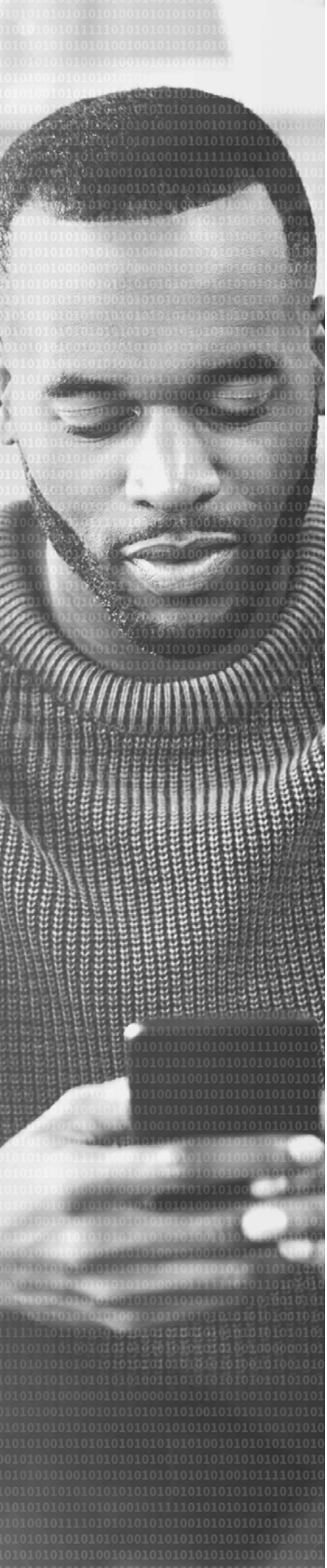


Fig.2: *Here we see activity from another mule account exhibiting notably different behaviours. After opening the account, there is very little activity for several months, before a sudden spike in activity. This is strong indication of mules preparing for the laundering activity. The mule makes arbitrarily low value payments to other mule accounts in the network to build a 'legitimate' transaction history whilst avoiding the banks' transaction monitoring controls.*



Witting mule accounts – i.e. these are accounts that knowingly send and receive fraudulent payments. They may begin as genuine customer bank accounts, but following an unseen prompt, suddenly or gradually become complicit in mule activity. Financially vulnerable groups such as students or those most affected by the cost-of-living crisis may knowingly give up their account details to criminal gangs in exchange for a cut of the funds.

Unwitting mule accounts – i.e. those who are transferring money without realising they are involved in laundering the proceeds of fraud. Often these are genuine individuals that are tricked into becoming a mule and moving funds with no awareness of the illegality of their actions. They may be victims of romance or investment scams, or believe they are legitimately employed as a 'money transfer agent', for example. Again, gangs will often target vulnerable groups – particularly students or those with financial worries – via social media with 'too good to be true' offers to make fast money without leaving home.

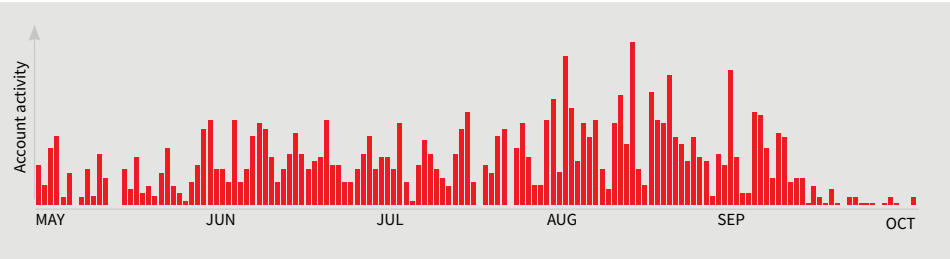


Fig.3: *This activity shows evidence of a once genuine customer, who later engages in mule activity. This is particularly hard to identify as the customer may have several years' worth of non-illicit activity. In this case, there was a notable change in behaviour: their 30-day average login volumes quadrupled and both payment volume and amount increased six-fold. Crucially, the volume of payments made to risky beneficiaries identified in the LexisNexis® Digital Identity Network®, also drastically increased.*

Mule herders extensively use social media to recruit new mules, often by flaunting images of exuberance and wealth on sites heavily populated by students, such as Tik Tok or Instagram. Paired with cleverly-wording advertisements, they encourage targets to get involved in 'legitimate' money-making schemes with no risk of reprisal. COVID and the UK cost-of-living crisis means more people than ever find themselves susceptible to such offers of a boost in income. Indeed, recent CIFAS figures show a notable increase in the over 30s being recruited as mules.

The challenge of deciphering between fraudulent mule activity and genuine customer transactions cannot be overstated. LexisNexis Risk Solutions, working alongside our banking customers, deploy a variety of strategies to tackle this problem, including data sourced from our global contributory database of transactional insights, the LexisNexis® Digital Identity Network®, as well as beneficiary account intelligence, UK Banking Consortium members, and advanced analytical techniques combined with custom models.

Machine learning mule model

In approaching the problem for Metro Bank in the UK, the team at LexisNexis Risk Solutions drew upon the latest modelling techniques and industry intelligence to deliver a solution that was not only capable of detecting mule activity effectively in near real-time, but doing so in a scalable manner that could be adapted to suit Metro Bank's changing requirements efficiently.

During the build, our expert Professional Services team of fraud data scientists worked closely with Metro Bank fraud teams, deriving first-hand insight from their investigations team that would ultimately help them to configure a solution to deliver optimum build and performance. Analysis of the data allowed us to identify key characteristics of mule activity that could be used to train the model to spot similar behaviours in a live account environment:

- **Ratio of inbound & outbound payments:** ('throughput') indicates the account holder is looking to 'wash' funds. Small values suggest tester payments.

Fig.4: *Equal value transactions*

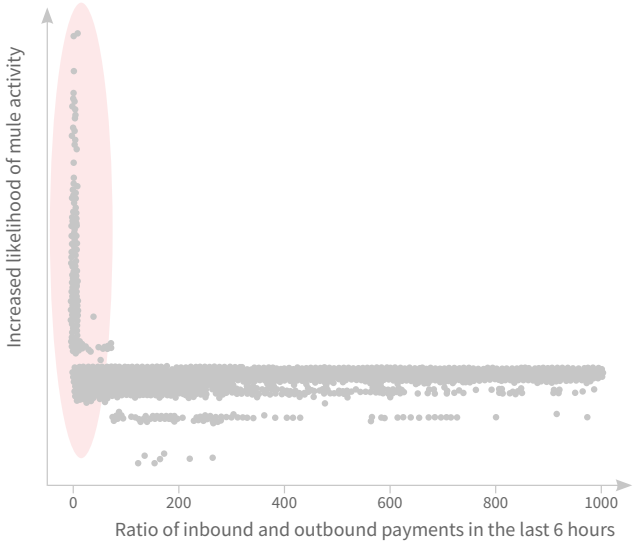


Figure 4 depicts all transactions assessed by the model, represented as grey dots. The x-axis gives the 'throughput' of the account (received funds versus sent funds over 6 hours), whilst the y-axis shows the risk attributed to throughput by the model. A higher y-axis value indicates an increased likelihood of money mule activity.

- **Higher-than-usual login activity:** where the mule account holder is continuously checking their account to confirm receipt of funds, prior to sending on.

Fig.5: *Higher-than-usual logins*

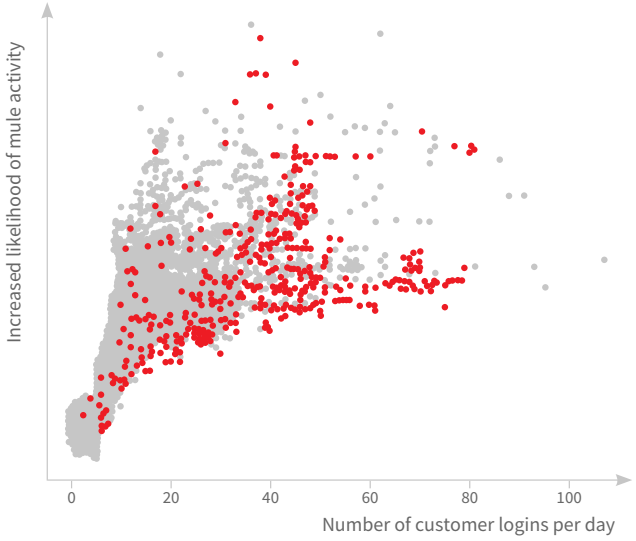


Figure 5 depicts all transactions assessed by the model represented as grey dots. The increasing concentration of red dots shows the number of unique beneficiaries paid by the mule. The x-axis shows the number of daily logins performed by the customer, whilst the y-axis shows the risk attributed to login volume by the machine learning model. A higher value indicates increased risk of money mule activity.

- **High volume of inbound payments:** utilising our networked intelligence we can monitor the volume and velocity of incoming payments from multiple banks into the same account over a 30-day period. This behaviour is highly indicative of an immediate beneficiary of scam funds.

Fig.6: *High volume inbound payments*

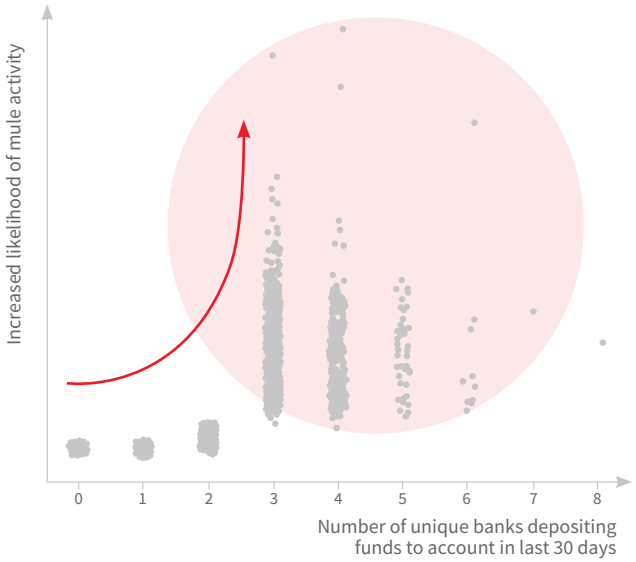


Figure 6 depicts all transactions assessed by the model, represented as grey dots. The x-axis shows the number of unique banks across our global network depositing funds into the account in the previous month, whilst the y-axis shows the risk attributed to inbound bank payments by the model. A higher y-axis value indicates an increased likelihood of money mule activity.

The model results

In just six months, using this trend analysis, the model successfully identified over £2.5 million of outgoing proceeds-of-fraud payments for Metro Bank, an uplift of 105% on previous fraud measures and representing over 20% of the total value of confirmed fraud payments detected over the period. In addition, one in eight (13%) of customer accounts flagged by the model over the period were analysed and later confirmed to be mules. Had these mule payments not been stopped, it would have been a significant cost to the bank under new PSR rules. However, with the full extent of unchecked mule accounts residing within UK banks being almost impossible to quantify, the total value of potential reimbursement losses is likely much higher and puts a strong imperative on banks to establish robust monitoring processes for both outgoing and incoming payments across their network.

The initiative has enabled Metro Bank to manage financial and reputational risk where there is a clear risk of money laundering, resulting in a broader reduction in successful first party fraud of up to 44%, equating to a 71% increase in historic detection volumes and landing a severe blow to fraudsters. Owing to the implementation of this model, Metro Bank can now successfully identify and resolve mule accounts far earlier, as well as mitigating any further suspicious incoming payments that could originate from an external fraud victim. In turn, this enables Metro Bank to greatly reduce the potential impact of the PSR's shared reimbursement rules.

Adam Glowaski, Fraud Analytics Manager at Metro Bank comments, *"Criminal gangs and the increasing prevalence of social media to recruit money mules is a key challenge. Ahead of the PSR's Mandatory Reimbursement, using smarter data and analytics to protect our business is vital to turn the tide by deterring money mules in addition to disrupting wider organised criminal activity."*

"Our partnership with LexisNexis Risk Solutions is providing the intelligence and adaptive solutions needed to identify fraudulent and/or high risk individuals, accounts, devices in addition to money mule networks."

Such is the success of this initiative; Metro Bank is already deploying a secondary machine learning model to complement existing strategies and further help identify behaviour patterns that might help indicate where customers have unwittingly become money mules.

For more information on how LexisNexis Risk Solutions can help detect money mules please get in touch by calling **029 2067 8555** or emailing **uk-irl-enquiry@lexisnexisrisk.com**

James Rushe
Engagement Manager

LexisNexis®
RISK SOLUTIONS

To find out how we can help you and your business,
call 029 2067 8555 or email uk-irl-enquiry@lexisnexisrisk.com

risk.lexisnexis.co.uk