Banks keep fraud details from police

Cash-strapped forces are not getting the help they need from secretive lenders — some of which even withhold funds from scammed customers

Ali Hussain

September 30 2018, 12:01am, The Sunday Times

Annabel Lee discovered by chance that Lloyds had £4,200 of her money, stolen several months earlier by scammers TOM STOCKILL

Police efforts to catch cyber- criminals are being hampered by a lack of specialist fraud investigators and banks' refusal to hand over details of suspect accounts, Money can reveal. Most forces have fewer than six officers dedicated to investigating banking swindles, a top fraud-buster has disclosed.

Norfolk constabulary does not have a single fraud specialist. It relies instead on detectives and officers who cover a range of crimes. In the 12 months to April last year, the force was sent 460 cases to investigate by Action Fraud, the national agency that logs cyber-crime and fraud reports from the public.

Dorset police has six specialist investigators. It received 316 Action Fraud referrals in 2016-17, suggesting each officer handles more than

50 cases, although non-specialists also handle such cases. Derbyshire constabulary has an 11-strong fraud team, but this is down from 16 officers in 2013.

In total, there are about 900 dedicated fraud investigators across the 43 forces in England and Wales, according to City of London police, which leads the effort to fight financial fraud. Those officers are dealing with as many as 70,000 cases and 70m documents.

Just over £500m was stolen by fraudsters in the first half of this year, according to the industry body UK Finance. Of this, £145m was lost to "authorised push payment" scams, where the victim transfers money to crooks in the belief that they are following instructions from their bank, the police or a trusted associate.

Even when police manage to identify suspect accounts that money has gone into, they may struggle to recover the stolen funds if banks refuse to help because of data protection rules. There is no standard procedure for banks to disclose account details to police — and some do not respond at all.

In a submission to the Commons home affairs committee in January, David Clark, who was temporary commander in charge of the police economic crime unit, said: "Timely access to this data will increase identification of offenders and money mules [where a fraudster persuades an account holder to receive stolen funds], secure evidence and victims' money, and increase the pace of action against fraud reports."

Requests for help were dealt with depending on banks' interpretation of the Data Protection Act, Clark said. "Some banks are very responsive, some take long periods of time to respond and others do not respond at all."

He pointed out that "a majority of regional fraud teams have fewer than half-a-dozen fraud investigators", which meant their capacity to deal with crimes was "not commensurate with the growth in threat".

Savers often fall victim to a notorious flaw in online banking. Conmen know banks do not cross-check the name on an account when a transfer is made: only the sort code and account number must tally. Last week, after growing pressure, the Payment Systems Regulator announced plans to require banks, by next April, to check the name corresponds too.

The consumer group Which? said last week a "shockingly low" number of cases are solved. Its research suggests 96% of crime reports to Action Fraud are closed without a successful outcome.

Kevin Hollinrake, co-chairman of the all-party parliamentary group on fair business banking, said the police "simply do not have the resources required to investigate the complex, mid-tier fraud cases. Banks need to stop hiding behind data protection rules and disclose information on fraudsters so the authorities can investigate and close them down."

Hollinrake urged banks to reconsider cases where refunds had been refused on the grounds that the victim had authorised a transfer to a fraudster. "It remains to be seen whether the banks will truly take a fairer view and whether they will do the right thing and consider old cases that have not been resolved," he said.

UK Finance said banks would "always work to provide information as quickly as possible but need to consider relevant legislation, including data protection rules". The group said it was working with the government and Information Commissioner's Office "on how to make this process easier and overcome some of the regulatory barriers that are hampering the fight against fraud".

City of London police said it was "reliant on voluntary co-operation from the banking sector", and in some cases lenders take "a significant amount of time to provide access" to account data.

It added: "We would like to . . . access this information quickly and work with banks more closely to share data that could . . . enhance police investigations."

Why don't banks return stolen funds?

About £130m is sitting in bank accounts set up by fraudsters. At present, this stolen money cannot be returned automatically to victims — their banks have to ask for it. This is because when a customer voluntarily makes a transfer, the money becomes the property of the fraudster — even if they were tricked into sending it.

"Banks don't have a legal obligation to return money to victims in all cases," said Paul Davis, retail fraud director at Lloyds. "In the case of authorised payment fraud, the money becomes the legal property of the account [holder] it has gone to.

"When banks take action to return the money, what banks are actually doing is breaking the terms of their own mandate with the fraudster and their account."

LLOYDS RECOVERED £4,000 OF MY STOLEN CASH BUT HID IT FROM ME FOR 16 MONTHS

If a bank recovers stolen funds, there is nothing requiring it to inform the victim or refund the money to them. Annabel Lee has waited 18 months for the return of more than £4,000 stolen online. It was only after she was alerted to it by police that she learnt the money was sitting in a Lloyds account.

Lee, who runs a printing business, received an email on March 9 last year, apparently from her business partner, asking her to transfer £8,670 to a firm they had worked with before. It gave a Lloyds account number and sort code.

"We were going through a major company restructuring at the time and there were many payments we had to settle, so it was not in any way an unusual request," said Lee, 54, from Chertsey, Surrey. She sent the money online from her Royal Bank of Scotland (RBS) business account. A couple of hours later, she received an email asking her to transfer £10,000 more to another account.

Lee became suspicious, then realised that the messages had come not from her business partner but an almost identical email address. She

immediately alerted RBS, which contacted Lloyds, but the latter said the money had left the scam account that day, so there was nothing it could do to help her.

What Lloyds did not disclose was that it had managed to freeze £4,203 of the money, which it had traced to a Nationwide account. Lee spent 16 months thinking she had lost all £8,670. Then, in July, a police officer told her that Lloyds had been sitting on the money all that time.

She rang the bank but was told it could not speak to her because she was not a Lloyds customer and she had to go through RBS. "It's almost as though Lloyds was hoping I would never find out about it," she said.

Lee became stuck in limbo because of a communication breakdown between the banks. After being contacted by Money, however, Lloyds said it would send her the £4,203 and would add £500 compensation.

Lloyds said: "Once notified [about the fraud] by her bank, we acted quickly to freeze the account and managed to reclaim funds that had already been transferred to another bank. Unfortunately, we did not notify Ms Lee's bank that these funds had been reclaimed.

"We apologise for the delay caused by this error and have been in touch with her bank to arrange for the funds to be transferred, along with an additional payment in respect of the distress and inconvenience caused by the delay."