Future of Banking – Tech trends

A SPECIAL 2-PAGE REPORT

Legal liability and the fight against fraud in the era of networked banking

Shifting regulations and a lack of clear jurisprudence put banks at fraud risk. A keen eye on both the law and technology can help them navigate these uncharted waters, writes **Jason Walsh**

The legal liability faced by banks in circumstances of fraud suffered by customers is at best opaque. A rapidly evolving area, the current 'Quincecare' legal principles go back to 1992, but are only now being put to the test in our interconnected era of electronic payments.

Stephen O'Connor, dispute resolution partner at Leman Solicitors, said the question is a complex one, and is being answered on a case-by-case basis. Like many elements of the law, it comes down to a question of balancing rights, he said.

Ronan McGoldrick, dispute resolution partner with Leman Solicitors said that the question remains open, but that banks need to understand the principles, even if those principles are currently being reviewed.

Some cases seem easy to answer, at least on the surface, but others can be unclear.

"Consider this scenario: a customer uses a public wifi network to make a money transfer in a café and as a consequence their computer is hacked. What if the hacker then fraudulently directs the customer's bank to transfer money or convinces the customer to transfer money? Who is liable? It's this type of scenario that regulations and case law in recent years have sought to address," McGoldrick said.

O'Connor said that there are generally three main scenarios when a bank could face liability: one is negligence on the part of the bank by failing to perform its duty of care, the second is breach of trust or fiduciary duty, and the third is the implied duty for banks to discover where a customer's orders are dishonestly given.

"A bank needs to be aware that an instruction to transfer money could be an instruction to commit fraud," O'Connor said.

Currently, the courts in England and Wales are the most active in creating jurisprudence which may in time be authority for the banks.

The Quincecare principles require a bank to exercise "reasonable skill and care" when executing the customer's instructions. Therefore, there could be a breach if there are reasonable grounds for believing a payment instruction is a fraudulent instruction. This duty is assessed against the objective standard of the ordinary prudent banker.

The original intention was that such a duty would strike a fair balance between placing too burdensome an obligation on banks to the detriment of necessary commercial banking activities and the need to protect customers against fraud.

Ronan McGoldrick, solicitor and dispute resolution partner, Leman Solicitors: 'Banks need to be alive to the kinds of payment instructions or requests that should raise red flags'

"Where the courts in England and Wales stand currently, is that the bank's duty to execute a payment is not absolute; it remains in tension with its duty of care to the customer," McGoldrick said.

In Ireland, banks are operating within a regulatory framework on the one hand and evolving case law on the other.

"It's obviously not an ideal situation," McGoldrick said.

"What is the bank supposed to do? And to what extent can it be proactive," McGoldrick said. "One possible option is for a bank to expressly contract out of the duties imposed on it by Quincecare. But having done so the bank would have to wait for the inevitable court challenge which will determine the legality of that."

Ultimately, globally, the future of banking is clearly digital, and this means a deeper approach to fraud detection will be an issue for banks, as it will be for other financial institutions. For instance, crypto currency fraud presents a new and daunting frontier. In 2021, crypto fraud cost the global economy US$21 billion (approx. €19.9 billion).

That figure will only increase and significantly so.

Technology has a significant role to play and banks are using progressively more advanced artificial intelligence to detect suspicious transactions.

> **A bank needs to be aware that an instruction to transfer money could be an instruction to commit fraud**

"It's not being used necessarily to look directly at individual transactions, but to look at the broader behaviour of the customer. Banks have invested heavily in AI and data-driven techniques generally and specifically in payments, as have other financial institutions," said McGoldrick.

"Banks still do need to be alive to the kinds of payment instructions or requests that should raise red flags," he said.

"Will the Quincecare duty be applicable in Ireland? Will the duty expand over time as it has since its inception in England and Wales? The jurisprudence that has arisen in England and Wales is still not settled. Many of the decisions have been a result of banks attempting to strike out a claim, but the court, or courts of appeal, say it needs to go to trial for clarification on what steps a bank needs to comply with. The future is still unclear, but there is a significant burden on banks," O'Connor said.

Data, due diligence and disruption

Data has the potential to unlock value and meet the growing regulatory challenge for the entire banking sector, from the incumbent players to new digital-only neo-banks, writes **Jason Walsh**

Heraclitus's refrain that 'change is a constant' has always been true, but the pace of change experienced in daily life has certainly gathered pace in recent decades. The unleashing of digital technologies, most notably data, has driven not only what can be done but also expectations of what should be done.

This is as true of customer expectations in banking and financial services as in any other field of commerce.

The question is: how can banks respond to the challenge? With the right partner they can respond with increasing speed, according to Tom Melville, group chief executive and head of CubeMatch Ireland.

"Customer demand is constantly changing. If you look at it now versus five or ten years ago, today everything is online 24/7. Legacy banks were certainly slow to respond to this," he said.

Indeed, the expectation today is that customers should be able to open accounts with just a few clicks – and this despite growing know-your-customer (KYC) and anti-money laundering (AML) regulations.

"Against that level of expectation, with traditional banks it often took two weeks to get approval for a mortgage," said Melville. Traditional banks are constrained by legacy issues. On the other hand, the neo-banks also face challenges.

"You've got two sorts of players: your traditional banks, with all of the legacy processes and paperwork, and the new digital-only, challenger banks. They both have challenges. For the legacy banks, it is that they have all of the people and controls in the background, but they need to become more agile. The challengers have the problem coming in the other direction."

For the moment, neo-banks are also able to enjoy the benefit of having a limited product offering: "They don't often offer mortgages and loans, or engage with that whole regulatory framework."

John Zoetekouw, CubeMatch Benelux's chief executive, said this was a major factor in how they were able to roll out services backed by IT systems that seemed smooth and flawless to customers. "The cost base is different: a fully digitised bank can have lower costs due to its smaller offering."

As they expand their operations, however, they will be forced to grapple with new challenges.

"KYC is important. A fully digitized bank, yes, they can now extend it to mortgages, but it can become more complex," Zoetekouw said.

Tom Melville, group chief executive of CubeMatch Ireland: 'Customer demand is constantly changing'
Mac Innes Photography

Data delivery

Indeed, opening a deposit account, transferring money and making payments are the easy services to roll out. Mortgages, business loans and complex financial investment products will require more data.

Zoetekouw said that, in fact, proper use of data was already required by central banks and regulators.

"When I started in the banking industry in the 1990s, you sent the regulator a report every three months. Now they want the raw data, and that will have an impact on your capital base."

On the other hand, data can help banks to deliver products and services as well as drive efficiencies – and bank data is among the cleanest, best structured and most useful data there is.

"Mortgage data, loan-to-value, information on your life, it all gives a lot of insight," Zoetekouw said.

However, accessing that data to drive insights is a challenge. "Most of our commercial banks have a history of 100 or 200 years, and usually they are a result of joint ventures and takeovers and mergers of hundreds of systems. As a result it's very hard to get an overview."

CubeMatch helps banks to do this by working with them to look at core data streams and ensure they can create key identifiers. "That requires time and discipline to make sure you maintain the key data."

Rapid access to data also has a compliance function: EU Single Resolution Board (SRB) rules mean that legacy batch processing systems will need to be upgraded or augmented.

"Under SRB, a bank needs to know its position within 24 hours of an event occurring. At the moment it's not real-time," Melville said.

In light of all of this, the decision on how to move forward requires looking at existing systems, the regulatory framework, business need and customer demands. "There's no one [single] solution because it depends on the complexity of the architecture."

Melville said that, as an international organisation with a long history in banking and financial services technology, CubeMatch was in a position to help banks understand their entire IT and regulatory footprint.

"What we've tried to do is cover all of the different things that meet our clients' needs. In Dublin we have the technology, in Amsterdam they have data science, and in London, risk analysis," he said.

In the end, though, Melville said CubeMatch's goal was to be seen as a partner, as that was how successful digital transformation projects were driven.

"The banks need to 'own' the projects themselves and put top people on it, and then bring in people to perform it."