DLA Piper is a global law firm with 4,200 lawyers located in more than 30 countries throughout the Americas, Asia Pacific, Europe and the Middle East. With one of the largest specialist banking and finance litigation teams in the world, we are well positioned to help companies with their legal needs, wherever, and whenever they need it. The UK team, which is made up of "dedicated and experienced banking and finance litigation practitioners" (Chambers & Partners UK 2013), acts for hundreds of financial institutions, including all the major UK clearing banks and provides advice and representation to banks, mortgage banks, building societies, finance houses, factors and invoice discounters and merchant acquirers as well as regulatory authorities.

In Practice

Authors Adam Ibrahim and Claire Clayton-Stead

Protecting the bank's position when customers fall hook, (on)line and sinker for vishing frauds

As fraud continues to cost the UK economy billions each year, bank customers are now looking to the banks to cover their losses. What steps should banks take to defend themselves against such claims?

Online banking fraud continues apace with the targeting of instantaneous online payment systems offered by all banks, which provide businesses with a swift and efficient payment capability. Common scams include "vishing" telephone calls, where customers are deceived into providing online banking security details, and viruses using harmful software to gather those details. With this information the fraudster effectively has a signed blank cheque against all the customer's online accounts and can misappropriate thousands – if not tens or hundreds of thousands – in a short space of time.

From the bank's point of view, these frauds often pass under the radar because, by virtue of the security information the fraudster has garnered, the bank has no way of knowing that it is not the customer undertaking the payments. Despite this, customers are turning to the law in their fight to recover fraudulent payments, yet their target is not the fraudster who has spirited their cash away, but their bank. The legal claims typically fall into three categories:

- Breach of mandate: the bank had no authority to make the payments.
- Breach of duty of care: the bank should have detected the payments were fraudulent.
- Claims for a refund under terms and conditions or the Payment Services Regulations 2009 (PSR) (SI 2009/209)

For once, the court of public opinion seems to be on the banks' side. The law, however, may not be so straightforward. At present, a bank's duty of care does not extend to detecting fraud on customer accounts (although there is a duty, once "on notice" of fraud, to halt transactions and alert the customer). However, given this law is over twenty years old, largely pre-dating online banking, it may be ripe for renewal by the courts so as to oblige banks, as a legal duty to their customers, to have fraud detection systems in place. This would have industry-wide connotations and place an expensive burden on the banking system, and despite the fact that all banks have invested heavily in technology such as real-time code-generating devices which provide far greater protection against fraud than was ever available in the days of cheque payments.

Furthermore, unless a bank's terms and conditions disapply certain of the PSR, banks must refund unauthorised transactions unless undertaken intentionally or fraudulently by the customer or caused by their gross negligence. Whilst there are certainly grounds to argue that disclosure by the customer of all their online banking security information is grossly negligent, there is presently no useful guidance – either from the courts or the FCA – on what constitutes grossly negligent conduct, leaving banks in a state of uncertainty.

There are, nonetheless, practical steps that can be taken:

- Ensure terms and conditions are clear about where responsibility for unauthorised payments lies and in what circumstances. They must also be PSR-compliant, and if banks want to opt out, it must be clear to which customers the opt-out applies and which of the PSR are being disapplied.
- The PSR state that any refund due is to be made immediately. FCA guidance suggests this means the same or next business day after notification of the fraud. If a refund is to be delayed pending investigation of the fraud, communicate this to the customer in the same timeframe and investigate promptly.
- Warn customers often and clearly about the hallmarks of online fraud and how to guard against it. The prospects of demonstrating that the customer was grossly negligent increase the more warnings and advice they can be shown to have received.
- Keep good records of activity on the customer's online banking facility: banks need to be able to evidence how the fraud occurred, especially since customers may not be able to recall or may be unwilling to admit exactly what information they shared with the fraudster.
- Have a voice-recorded fraud-reporting telephone line to capture any helpful early disclosures customers make about the information shared with the fraudster.
- Have in place procedures to contact third party banks swiftly to maximise funds recovery. The faster this contact, the greater the recovery and the lower the prospect of the customer claiming against the bank.
- Communicate regularly with customers during any investigation: litigation often arises as much out of customers' dissatisfaction with how their case has been handled as out of the underlying circumstances of the claim.

In short, in the face of the current legal uncertainties, banks should do all they can to control the limited factors within their control, to protect against claims. Whether that is enough will have to be determined by the courts and the FCA. ■

Biog Box

Adam Ibrahim (partner) and Claire Clayton-Stead (associate) are members of DLA Piper's litigation & regulatory team specialising in banking litigation, including online fraud and cyber-crime. E-mail: adam.ibrahim@dlapiper.com and claire.clayton-stead@dlapiper.com