NEW SQUARE

LEGAL Analysis

OCTOBER 2018

APP and Cyber Fraud:
a Commercial Litigator's Perspective

About the author

SHAIL PATEL

Shail Patel is a commercial litigator with a particular focus on financial services, fraud and insurance. He also advises in regulatory and disciplinary investigations and enforcement proceedings.

"He is smart, technically very good and provides watertight advice. He is also very good with clients." "Very intelligent, switched-on and on the ball commercially." *Chambers & Partners, 2018*

Introduction

APP ("authorised push payment") fraud and related cyber frauds have featured heavily in the financial and mainstream press lately. These scams involve the victim being tricked into making an instant electronic payment to fraudsters instead of the intended recipient.

The industry has taken note, and a voluntary code for Payment Services Providers is currently under consultation. If it is adopted in 2019, it will provide for compensation for certain victims in certain circumstances. However it is unlikely to assist those who have already fallen victim, and it may not assist SMEs and larger businesses.

The average loss in APP scams in the first half of 2018 was around £10,000. Those cases do not get anywhere near the desk of the commercial litigator. However some criminals set their sights higher, and losses ranging from £250k to several £m are increasingly common. In those cases the question of civil recovery against parties involved in the transaction can loom large.

While big money cases will justify expensive freezing and asset tracing exercises, in many cases this will be both prohibitively expensive, and too late; experience shows that when the money is gone, it moves fast, splits up and ripples quietly through the financial system. This article is concerned with other routes of civil recovery in cases where some initial investment may prove very worthwhile; not only in legal advice, but also specialist IT forensic investigation, to establish what has gone wrong and who might be to blame.

A Galaxy of Scams

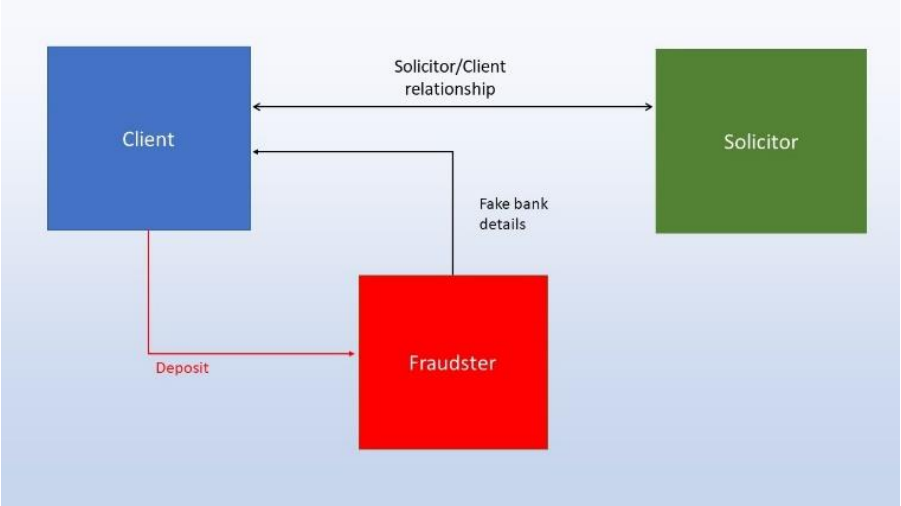
In the most basic example of APP fraud, the victim simply asks his own bank to pay a fraudster instead of (say) for his ski holiday. Such cases will require regulatory and industry intervention because there is little room for litigation.

However, it is clear that fraudsters are targeting a greater array of transaction types to bag the biggest windfall gains. From more modest thefts of school fees and kitchen orders, they are seeking to divert substantial payments intended for property, currency and commodities to name a few. Importantly for the purposes of civil recovery, deep pocket defendants can become caught up in the fraud.

The methods of deception increasingly involve convincing "social engineering" (essentially confidence tricks and impersonation) combined with sophisticated manipulation of electronic communications, over a long period of time. It is common to see a victim talking to an impostor by email for weeks or months prior to payment.

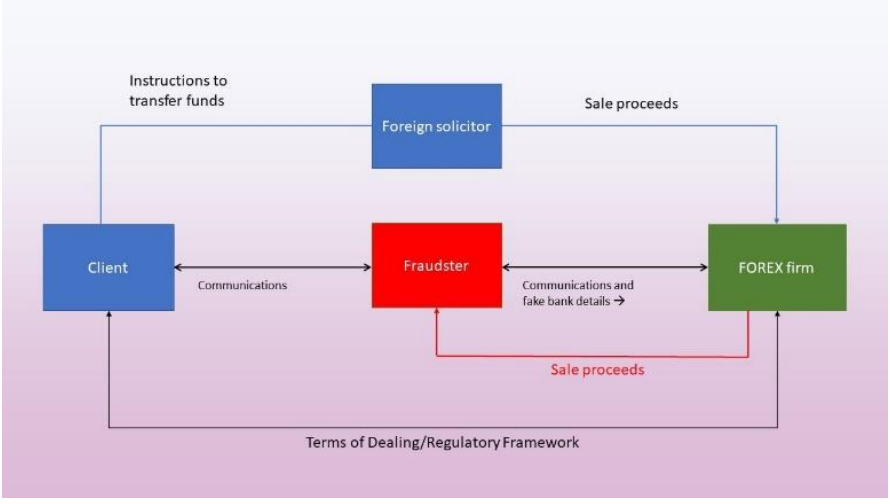
The following examples are based loosely on cases I have come across. The expression "client" is used for convenience to refer to the potential claimant.

Example 1:



In this example a purchaser is tricked into paying cash to a fraudster instead of his solicitor. The solicitor might equally be an investment manager or broker looking to invest funds for the client. The common thread is the backdrop of a professional-client relationship.

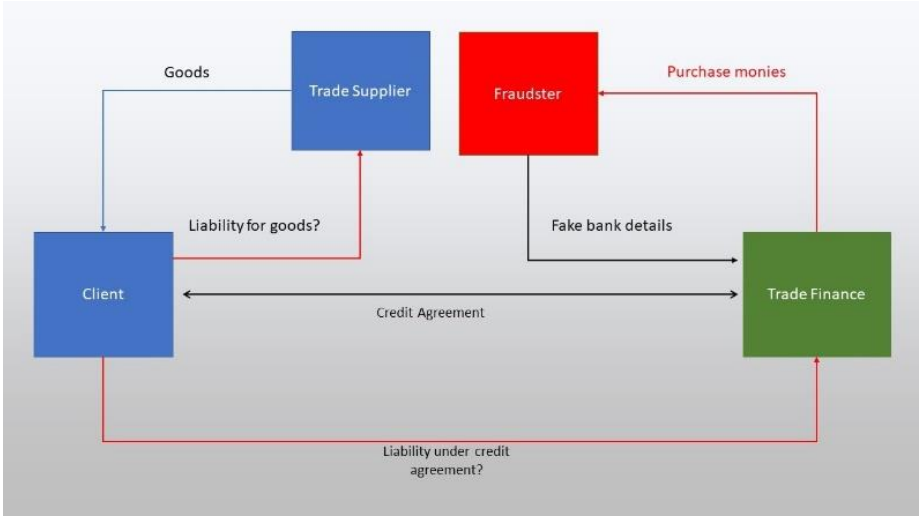
Example 2:



Here the fraudster has interposed himself in a transaction to convert the sale proceeds of a foreign property into his domestic currency. In one case the fraudster simply provided fake bank details, but in another the fraudster conducted an elaborate personality scam,

whereby both the client and firm dealt almost exclusively with him alone. The fraudster 'mirrored' some communications and manipulated others, ultimately providing a fake explanation for the use of the funds in a seemingly unconnected jurisdiction. Importantly, the monies were paid out to the fraudster from the bank account of the FOREX firm.

Example 3:



Here the fraud is directed at another triangular relationship; a wholesale transaction negotiated between the client and the supplier for good or commodities. The payment by the finance company to the fraudster creates two major problems for the client; a potential liability to his trade finance lender for the amount paid out, and a liability to the supplier for the goods (or potentially the difference between the contract price and the value of the goods if the supplier seeks damages). In cases of this nature (and in example 2) identifying the 'victim' of the fraud is not so straightforward, and the right 'moral' allocation of the loss between victims can be less than clear.

Issues to Consider

The headings below cover some issues to consider when formulating recovery strategies in these sorts of cases. The common law on APP fraud is almost entirely undeveloped, giving practitioners the opportunity to be creative.

A Professional/Client Relationship

In contrast to parties in an arms' length transaction, if the overarching relationship between the client and another person caught up in the fraud is akin to a 'professional/client' relationship, there are likely to be implied duties of care and skill (s.13 of the Supply of Goods and Services Act 1982 and s.49 of the Consumer Rights Act 2015) and potentially fiduciary duties owed. Moreover, when the professional operates in a regulated sphere, such as a financial services professional or a solicitor, there are both rules to comply with and industry knowledge, learning and guidance, which the client can argue that they are fixed with.

So taking example 1, the client can argue that as between himself and the solicitor, the latter should have been aware of (e.g.) the longstanding Law Society warnings and guidance on APP and cyber fraud and should have taken some reasonable steps to protect its client from a scam which is well known to conveyancers, but not an average property purchaser (who might only transact every few years). The prevalent email footers now included in solicitors' emails, warning the recipient not to accept bank details by email, are a telling indication about the scale of awareness of the problem.

Sophisticated financial institutions commonly use online platforms with passwords and login credentials to facilitate payments. While using these is generally secure, the position of an institution which is willing to communicate by email and even permit payments outside of the platform could be unhappy. It raises the question; if the platform is thought necessary for cyber-security, how could it be appropriate to deal with customers outside of the platform by any non-secure method such as email? Given the prevalence of APP fraud in the financial sector, what duties (including arising from the FSMA regulatory regime, the principle of care and skill, etc.) are there to give warnings to customers, or even potential customers, about the risk of bogus communications? These are largely uncharted waters, and arguments along these lines cannot be dismissed out of hand by a sophisticated defendant caught up in a fraud on a layperson or business.

Contractual Allocation of Risk

In the above examples, there may be contractual terms of dealing between the client and the potential deep pocket defendant. Experience shows that even in 2018 it is rare that the latter's standard terms of business will cater for anything like the eventuality of APP fraud. Many businesses are, unfortunately, well behind in considering and allocating the risk of APP fraud. Until they do, that is an opportunity for a claimant/victim, and a risk for such firms.
For instance, in examples 2 and 3, a question arises regarding the basis on which the potential deep pocket defendant is entitled to accept instructions to make a payment. If it accepts instructions to make a payment from someone other than the "client" - even if masquerading as the client - its own contractual terms may leave it in a difficult position unless they expressly address the question of impostors or 'reasonable apprehension'.

If the contractual terms couch liability in the language of "negligence" it may become necessary to consider whose fault it is that the parties were exposed to the fraud. IT forensic investigation can usually establish which email accounts have been compromised (which is almost always the first step to APP fraud, as fraudsters need to delete incoming emails from the genuine payee and some outgoing communications that might alert him to the fraud). Establishing *how* the account was compromised can be more difficult however. If an employee has simply left his computer unlocked and it is accessed, that may be negligent, but if he has disclosed his password in a convincing phishing attack, the conceptual framework of 'negligence' becomes more difficult to apply. It can certainly be argued that a sophisticated institution or professional could be expected to achieve a higher standard than a lay person in this regard.

Dreamvar and the new landscape for breach of trust

If the APP fraud is perpetrated on someone holding the client's money, his position is potentially rather better. Of course a bank does not count, as a bank account is a debt rather than a trust of money. However a solicitor's or financial firm's client/segregated monies account is intended to maintain the client's title to the funds. The funds are therefore held on trust by the firm for the client.

Traditionally a firm who is induced by a fraudster to make a payment out in breach of trust would have relied on s.61 of the Trustee Act 1925, entitling him to relief on a discretionary basis, provided he had acted reasonably and honestly. Thus if a firm had been carelessly duped, it would likely be on the hook - but if it had complied with its duties and regulatory obligations and been duped by a sophisticated fraud, it would not.

This orthodoxy has been disrupted by the High Court's decision in *Dreamvar v Mishcon de Reya,* upheld by the Court of Appeal (on the relevant point) in May of this year ([2018] EWCA Civ 1082). MdR acted for the purchasers in a transaction where the vendor of a London property turned out to be a fraudster who did not own it. The High Court found that MdR had acted in breach of trust in paying the money out, and although they had acted honestly and reasonably in doing so, they were refused relief under s.61. This was on the basis of policy alone; the purchaser was small, the purchase price was entirely lost, the purchaser had no insurance to protect from such eventuality, whereas MdR did. Thus MdR was far better placed to absorb the loss.

Of course every case turns on its own facts, but the significance of that decision in APP fraud cases involving lost trust monies is surely great. Until first party cyber fraud insurance becomes routinely available and adopted, the firm (be it professional or financial regulated firm) will be much better placed to absorb the loss.

Residual bank claims

In APP fraud cases, claims against the banks involved are usually difficult. However there are potential legal routes which might be available on the right facts.

In *Singularis v Daiwa* [2018] 1 WLR 2777 the Court of Appeal upheld a finding that a bank was liable for payments out from the claimant's account when there were glaring indications that the payments were fraudulent. This was a manifestation of the "*Quincecare"* duty, named after *Barclays Bank v Quincecare* [1992] 4 All ER 363. In *Singularis* the fraud was perpetrated by a director of the claimant by making wrongful payments out of its account.

The *Quincecare* duty is exceptional, and a claimant will have to surmount a high hurdle to show that the bank was sufficiently on notice of fraud. Where the client has simply instructed his bank to make a payment to the wrong bank account, the bank will have no reason to know that the instruction was procured by third party fraud. However, what if the payment was highly unusual in its amount or nature? Banks habitually stop overseas card payments where fraud is suspected, though it is rarer in cases involving BACS or CHAPS. Nevertheless if a bank does comply with instructions to pay an unprecedented (for that client) sum out of a customer's account to an offshore or foreign bank, *Singularis* provides the kernel of the argument.
What about the bank who receives the funds? It is not unusual that the recipient bank account will have been recently set up, and will have had little or no activity other than receiving the proceeds of the fraud. A question arises about the extent to which that recipient bank complied with its KYC and AML obligations (and indeed what those obligations are in the relevant jurisdiction). Whether such a bank owes a common law duty to comply with those regulatory obligations, to potential victims of cyber-fraud, is an interesting moot question, and an area which is surely ripe for development.

Conclusion

As can be seen, a victim of a substantial APP fraud is not always high and dry. Some creative thinking might be needed to identify targets for mitigating the loss and formulating claims against them. However the changing nature of APP frauds, in ensnaring a greater number of (potentially) deep pocket participants, tends to increase the prospects of recovery.

As a post script: the industry's response to APP fraud is not the subject of this article; though it is worth noting that there is little appetite to assist SMEs or larger businesses. A useful summary of the general response as at June 2018 can be found in this practice note from Matt Hancock at Mishcon de Reya.

To read more about the Payment Service Providers' draft code and 'contingent reimbursement model' announced on 28 September 2018, click here.

The FCA is consulting on bringing APP fraud within the jurisdiction of FOS; click here for more details. Of course this will only help consumers and micro-enterprises.