

The Jackson Reforms

This year's hot topic – for experts and solicitors alike – has been the requirement for expert witnesses to provide cost estimates, under the revised Civil Procedure Rules which came into effect in April following Lord Justice Jackson's report into civil litigation costs.

Cost estimates have in fact already been required for some time by firms on large insurers' panels or working under a contingency agreement or "After The Event" cover. We recognise the need to assist instructing firms in responding to the new costs regime and are organised to engage with the new requirements. A word of caution, though - while we can set out costs estimates on a clear and systematic basis, we do not have a magic formula

for predicting the time required in complex financial disputes, especially those where an expert may need to work through several bundles of documents to establish which are or are not relevant.

The Jackson Reforms have prompted us to publish a series of short briefings on the major areas on which we are approached. Instructing lawyers may find these helpful in establishing what types of expertise are needed and what areas are commonly addressed. Please see overleaf for further details.

Paul Rex

Managing Director
GBRW Expert Witness
August 2013

Tim Dowlen joins GBRW Expert Witness

We are very pleased to announce that Tim Dowlen joined GBRW Expert Witness as Director, Insurance earlier this year. Tim is a divisional director of a City-based Lloyd's broking firm, Tasker & Partners, where he is responsible for developing the firm's retail insurance activities. He has been a director of insurance broking companies since 1973 and was for many years the Senior Examiner in Liability Insurance to the Chartered Insurance Institute. As a practising expert, he has given evidence in more than 100 cases and was one of the Principals of Associated Insurance Experts at the time of its acquisition by GBRW Expert Witness.



Areas of Expertise include:

BANKING & FINANCIAL:

- Corporate Lending
- Personal Lending
- Risk Management
- Investment Banking
- Corporate Finance
- International Banking
- Correspondent Relationships
- Commercial Property
- Residential Mortgages
- Syndicated lending
- Loan Workouts
- Recoveries and Realisations
- Back Office Procedures
- Trade Finance
- Letters of Credit
- Leasing
- Credit and Debit Cards
- Know Your Customer
- Anti Money Laundering
- Anti Terrorist Financing

INVESTMENT MANAGEMENT

- Investment Services
- Investment Advice
- Fund Management
- Structured Investment Funds
- Stockbroking
- Hedge Funds
- Options, Swaps, Derivatives
- Treating Customers Fairly
- Pensions

FINANCIAL MARKETS:

- Money Markets
- Commodities Markets
- Securities Trading
- Financial Instruments

INSURANCE:

- Property Insurance
- Professional Indemnity
- Life Assurance
- Broking
- Underwriting
- Reinsurance
- Regulation
- Actuarial issues
- Loss Adjustment
- Treating Customers Fairly

BUSINESS FINANCE:

- Limited Companies
- Partnerships
- Private Companies
- Sole Traders
- Mergers & Acquisitions
- Treasury Management
- Sales of businesses
- Property Finance
- Business Planning
- Company Valuation
- Venture Capital

OTHER AREAS:

- Employment Disputes
- Loss of Earnings
- Compensation Calculations
- Arbitration and Mediation

Enquiries:

Paul Rex,
Jeremy Denton-Clark
or David Croft
T: 020 7382 9900
F: 020 7382 9988
E: experts@gbrwexpertwitness.com





Electronic payments – what happens when things go wrong?

Richard Palette has nearly 40 years experience in retail financial services, banking operations and internal audit and was Head of Professional Practices, Group Internal Audit at RBS prior to his retirement in 2009. Richard has worked for us as an expert on several cases involving electronic payments fraud and shares his experience below.

Background

Electronic payments between bank accounts of companies and private individuals have been with us for many years. Most of us are familiar with BACS, CHAPS and SWIFT and, since 2008, Faster Payments. Most of us also routinely use online banking on PCs, smartphones and other mobile devices to make payments to third parties. In other words, the payment industry has developed rapidly away from historic paper based methods of payment using cheques.

To cope with this increase in the use of electronic payment systems, UK banks have developed increasingly sophisticated means of protecting users against fraud. At the same time, their terms and conditions for users of payment systems have become increasingly complex and in corporate banking, ever more slanted in favour of the banks should problems arise.

Whilst large numbers of payments are routinely processed without problems each day, what can go wrong and what issues are raised when fraud occurs?

Fraud patterns

We have seen a number of cases recently where businesses have been defrauded by a trusted employee in charge of paying a company's bills. The standard modus operandi is that the fraudster substitutes his or her own sort code and account number in the payment instruction, while retaining the name of the true beneficiary (usually a company).

To the surprise of many, the banks' payment systems do not take a beneficiary name into account when processing a payment. The systems work on what is defined in the Payment Service Regulations as a 'unique identifier' which in the case of inland payments between UK banks is a combination of the sort code and account number. The cost to the banks of changing

systems to recognise account names as well as numbers is regarded as prohibitive.

Not unreasonably, the banks' terms and conditions require companies to have their own anti-fraud controls in place - including not allowing unauthorised access to passwords, PINS and authenticators. However, when it becomes clear that an authorised employee has abused their position of trust, customers ask what their bank's responsibilities are in this situation. Should a bank not be required to notify its customer when a large volume of payments is being made regularly to the same sort code and account number but with different beneficiary names? The answer is quite unsatisfactory from a customer's viewpoint.

Anti-Money Laundering Regulations

Banks have obligations under Anti-Money Laundering (AML) regulations to monitor customer accounts and to be suspicious of any activity that does not fit the pattern expected from its knowledge of the customer. If a customer in a clerical job earning £20,000 a year receives multiple credits totalling tens of thousands of pounds from the account of his or her employer, this should raise suspicions. Funds are often withdrawn rapidly (sometimes as payments to gambling organisations), which should heighten suspicions.

Banks understandably take a risk based approach which focuses on high risk accounts and larger sums than often feature in frauds of this kind, but that does not absolve them of their AML responsibilities.

However, it is important to bear in mind that the bank conducting the AML monitoring is the fraudster's bank, not the defrauded party's - when things do go wrong, its first response is to deny any liability to the originator of the payment(s). In one recent example, the bank holding the account of a subsequently convicted fraudster actually wrote to him advising that payments not bearing his name, but those of third parties, had been received into his account. The bank felt it had no further responsibility to any other party.

What is the legal position?

Surprisingly, there is no case law that sets precedent in this area. While cheques are covered by statute dating back to 1882

and it is a long established principle that banks should not collect cheques payable to anyone other than the payee, there is little protection currently available to those who suffer fraud from electronic payments.

As a result, customers who have been on the receiving end of this type of fraud have limited scope for claiming against their bank. They may be able to negotiate some compensation from their own bank if it also holds the fraudster's account, or from the fraudster's bank when AML procedures have not been properly followed, but this depends on the bank's reluctance to suffer adverse publicity rather than on a legal basis for a claim.

Whilst it would be unreasonable to hold banks responsible for reckless or careless use of security procedures by customers, they are nonetheless in possession of detailed information regarding activity through the accounts of both payer and recipient. With better use of this information, identification of fraudulent payment patterns could be brought about much earlier. In the absence of statute, it is perhaps time for the courts to look at this important aspect of commercial activity in the context of today's technology and business practices.

In the meantime, the best safeguard is to ensure that a second pair of eyes scrutinises all account activity on a regular and systematic basis.

Subject Briefing Papers

GBRW Expert Witness has launched a series of Briefing Papers to provide general background on the topics on which we are approached most often. The series currently includes:

- Instructing an expert
- Investment disputes
- Interest Rate Swap disputes
- Commercial property lending disputes
- Trade Finance disputes
- Insurance disputes

with more to be added shortly. The Briefing Papers can be downloaded from <http://www.gbrwexpertwitness.com/Expert-Witness/briefings>.

...there is little protection currently available to those who suffer fraud from electronic payments....