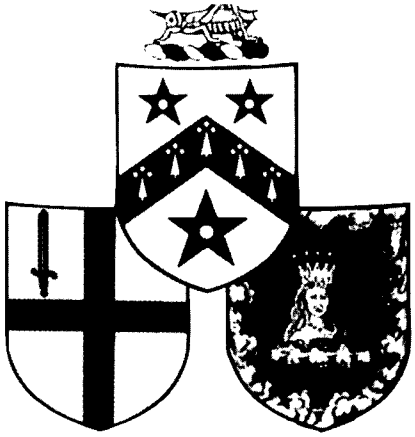
G R E S H A M

C O L L E G E



WORLD CYBERSPACE LAW

Lecture 3

CYBER/CONTRACTS

by

PROFESSOR GERALD WAKEFIELD
Gresham Professor of Law

9 December 1999

INTERNET FRAUD

Advances in Telecommunications during the latter half of the twentieth century have provided enhanced commercial opportunities. It is estimated that approximately $US500 million dollars worth of transactions took place on the Internet in 1995. By 2005 global online commerce is expected to reach between $US76 billion and $US186 billion.

Internet Fraud

Because it cannot be effectively regulated and controlled, the full extent of Internet fraud cannot be determined.

In the US, the National Consumers League ("NCL") collects and disseminates information relation to fraud on the Internet, . That information is illuminating and provides at least anecdotal evidence of what may be occurring in the UK on a limited scale or what the UK may expect.

The NCL, in its remarks to the US Senate Permanent Sub-Committee on Investigations on 10 February 1998, reported that email enquiries to it had increased ten fold since the inception of its internet fraud watch program. And reports of possible Internet fraud had tripled from an average of 32 per month in 1996 to nearly 100 per month in 1997.

The most common categories of complaint to the NCL in 1997 were as follows:

- Web auctions where items bid for were never delivered by the sellers, the value of items were inflated and prices were increased after bids were accepted;
- Internet services involving charges for services that were supposedly free, payment for online and internet services hat were never provided or falsely represented;
- General merchandise sales of everything from t-shirts to toys, calendars to collectables, which were never delivered or delivered not as advertised;
- Computer equipment / software where computer products were never delivered were misrepresented;
- Pyramid schemes which profit from recruiting others, not form sales or goods or services to the end users;
- Business opportunities / franchises which promise big profits for little or no work and involve investing in pre-packaged businesses or franchise operations;
- Work at home plans which sells materials and equipment with false promise of payment for piece work performed at home;

- Credit cards falsely promised to people with bed credit histories on upfront fees;
- Prize / sweepstakes that request up-front fees to claim winnings that were never awarded;
- Book sales in subjects such as genealogy and self-improvement that were never delivered or were misrepresented.

The common elements of each of the top ten subjects of reports referred to above are request for advanced payment for sellers with whom the consumers are not familiar, who were usually located in another state, or even another country, and who were usually located in another state, or even another country, and who have made exaggerated claims or false promises concerning the goods or service offered.

The immediate victims of Internet fraud are the consumers who have paid for goods and services promoted through the Internet and who have not been provided with what they have paid for. Where providers of goods and services on the internet exhort the use of credit cards as a means of payment, credit card companies and the lending institutions which issue those cards may also sustain significant losses through internet fraud where consumers have paid for goods and services by the use of credit cards.

Remedies

Jurisdictional Issues

Laws are drafted on the premise that their jurisdictions is confined by geographical and political boundaries. It is not possible, in any traditional sense, to regulate and Internet transaction in which, for example, the buyer, seller and linking servers may each be in different countries.

A further complication occurs where a dispute may arise over an Internet transaction. Commercial disputes are normally determined by a Court which has a territorial jurisdiction connected in some fashion to the site of the alleged wrongdoer's act or omission. But where does a relevant act or omission, for example fraud, take place where the transaction is consummated via the Internet?

When an individual logs on to the Internet an electronic presence on the net can be detected by a wide variety of computers linked to the Internet from virtually anywhere in the world. As a jurisdictional matters, where does an alleged wrong take place?

Is it where the presence is received?

Is it as the place of logging on?

Or is it in the jurisdictions of each of the computers in which the electronic presence is detected anywhere in the world?

This is a difficult question to answer and is an issue that will inevitably arise for determination in disputes involving e-commerce.

In *CompuServe v Patterson*, 89 F.3d 1257 (6th Cir. 1996), the United States Court of Appeal for the sixth circuit had to determine whether CompuServe could sue one of its subscribers in Ohio (the site of its corporate headquarters) even though the subscriber was from Texas and had never physically been to Ohio but had visited, so to speak, CompuServe in Ohio by using the internet.

CompuServe brought a suit in its home state of Ohio against an individual who lived and worked in Texas and developed shareware. The Texas software developer sold and marketed his shareware over the Internet via CompuServe's shareware servers. He used the CompuServe service by modem from his home computer in Texas and he subscribed to CompuServe via that modem connection.

The Texas shareware developer sent several messages to CompuServe through e-mail, claiming that CompuServe software products infringed his rights. The e-mail message originated form the shareware developer's desk in Texas and arrived at

CompuServe's Ohio headquarters. Because the Texas developer used the CompuServe shareware service, Internet surfers who downloaded his software got it from a CompuServe server in Ohio.

In a pre-emptive strike, CompuServe sued in Ohio for a declaration by the Ohio Court that CompuServe had not violated the Texan's rights. Obviously, for the Texas shareware developer to assert those rights he was required to either prove his case in Ohio or convince the Ohio Court that it lacked jurisdiction to decide the issue.

The Texan shareware developer argued at first instance that he had never been to Ohio and that the only connection that he had at all to Ohio was the fact that CompuServe happened to be there. The Court at first instance held that it did have jurisdiction. The Court of Appeals found that the Texan shareware developer's electronic visits to Ohio subjected him to the jurisdiction of the Ohio Courts.

In delivering its judgement, the Court of Appeals stressed that the Texas shareware developer "consciously reached out from Texas to Ohio to subscribe to CompuServe and to use its service to market his computer software on the Internet".

Further, it found that he "originated and maintained contacts with Ohio" when he e-mailed CompuServe at its Ohio headquarters about his claims. The Court acknowledged that it may "burden some for [the Texas shareware developer] to defend the suit in Ohio, but he knew when he entered into [the agreement] with CompuServe that he was making a connection with... [Ohio]."

The rationale of CompuServe regarding jurisdiction is that it is arguable. This is similar to the rule governing when and where a contract is concluded in circumstances where acceptance is to be by telephone, telex or some other instantaneous form of communication. The contract is concluded when and where the message is received.

Jurisdictional issues could therefore be a significant obstacle to victims of Internet fraud seeking to pursue remedies against the perpetrator of fraud. These concerns are probably limited to direct victims of fraud. A credit provider whose only connection to a fraud is through the provision of a merchant facility to the fraudster will usually have some geographical connection with the fraudster. But this is no guarantee of recovering monies paid by a credit provider to victims of its customer's fraudulent conduct.

Contractual remedies

A victim of Internet fraud who has paid for the goods and services by credit card is likely to seek compensation form the card issuer concerned pursuant to the standard terms and conditions of the card.

If the complaint by the victim is verified, the card issuer is compensated by the issuer of the merchant facilities, the card issuer will normally credit the victim's account with the full face value of the subject transaction.

Under the terms of most merchant facilities, the card issuer is compensated by the issuer of the merchant facility is concerned. The issuer of the merchant facility, as the issuer of the facility to the fraud or scam artist, is then left with the unenviable task of charging back disputed transactions to its customer's account and recovering those monies.

Well-run scam operations are usually difficult to identify. More importantly, their assets will either not be available in the relevant jurisdiction or if they are, cannot be attached for execution.

Therefore, while a credit provider in the form of the issuer of a merchant facility may have contractual rights against its customer under the terms of its merchant facility, those rights, on close analysis, may be worthless.

Tracing

Tracing is a remedy available both at common law and in equity. It describes a process enabling a plaintiff to seek to recover monies taken or assets acquired with the proceeds of a wrongful act, such as the perpetration of a fraud.

Tracing at common law is available where it can be established that a defendant has received the plaintiff's money, and therefore, the extent of the defendant's liability will be determined by the amount of money received. Liability depends on the receipt of the money rather than its retention. The main limitation of tracing at common law, however is that once monies have been mixed with that of others, the remedy is lost.

The cost of tracing exercise is prohibitive to most people, especially those consumers who have been defrauded for relatively small amounts of money through one or other of the many scams being perpetrated on the Internet. Therefore, while the remedy may be available, it is of little practical use.

Tracing at common law will provide little if any remedy to a credit provider who has compensated a victim of credit card fraud because there is no relationship or nexus either in contract or tort between the credit provider and the fraudster. Such a relationship

is necessary to invoke any common law remedy including tracing at common law.

Tracing in equity also has it limitation. There is a view that tracing is only available where some pre-existing fiduciary relationship can be shown. Tracing in equity generally arises when a trustee converts trust property to his own use. In such a case, the trustee, who is clearly in a fiduciary relationship with the beneficiaries, is liable to account to the beneficiaries for the trust assets converted by him.

The view that an antecedent or pre-existing fiduciary relationship must be shown has been the subject of criticism.

There have been cases where tracing in equity has been permitted even though there was no antecedent fiduciary relationship. In these cases courts have held that the knowing receipt of assets representing misappropriated funds, constitutes the recipient a trustee and subject to the proprietary remedy of tracing by any victim of the fraud, because the victims are entitled in equity to a return of the monies paid to them.

It would therefore appear that assets acquired with monies form the victim of a fraud are able to be traced in equity. For the reasons referred to above in the discussion of tracing at common

law, tracing in equity is also unlikely to provide an effective remedy to a defrauded customer.

Is tracing in equity available to a credit provider who is not a direct victim of the fraud but only indirectly involved by virtue of the fact that it has compensated the victim? There are no cases of which I am aware where this issue has been determined. However, it is arguable that a credit provider who compensates a victim of fraud should be subrogated to that victim's rights as against the fraudster to seek recovery from the fraudster of the monies paid by the credit provider or assets obtained by the fraudster with those monies.

As subrogation is a creature of equity with natural justice origins, the principle should extend to allowing a credit provider to seek redress from a fraudster where it has compensated the victim of a fraud.

Conclusion

The development of the Internet and the proliferation of e-commerce have spawned a new class of fraudster or scam artist which have been collectively described, by one commentator, as the "information super highway-men". The Internet is here to stay and the challenge ahead for consumers is to stay one step ahead

of the fraudsters. As consumers we can achieve this by exercising a little common sense and discretion in our e-commerce dealings.

The challenge ahead for credit providers is to service this rapidly growing industry while minimising the risks of dealing in it.

Neither consumers nor credit providers can rely on governments to provide effective regulation of the Internet. Cyberspace, or its nature, is not amenable in any effective sense to government regulation and control.

The traditional remedies available may or may not be adequate in the circumstances. Only time will tell. In any event, those remedies may be rendered practically nugatory die to the jurisdictional issues which are likely to arise and the availability of assets in the relevant jurisdiction to which a judgement against a fraudster may attach.

In the absence of effective government regulation and effective legal remedies, it would appear that public education must be a major component of any effort to curb Internet fraud. Consumers need to be educated, primarily, on how to identify fraud on the Internet so as to not fall victim to it. Credit providers can play a role here by scrutinising applications for merchant facilities very carefully, especially merchants who intend to conduct business

over the Internet. These measures may reduce substantially the risks of Internet trade to the mutual benefit of the consumer, the merchant and credit providers alike.

GRESHAM COLLEGE

Policy & Objectives

An independently funded educational institution, Gresham College exists

- to continue the free public lectures which have been given for 400 years, and to reinterpret the 'new learning' of Sir Thomas Gresham's day in contemporary terms;

- to engage in study, teaching and research, particularly in those disciplines represented by the Gresham Professors;

- to foster academic consideration of contemporary problems;

- to challenge those who live or work in the City of London to engage in intellectual debate on those subjects in which the City has a proper concern; and to provide a window on the City for learned societies, both national and international.

Gresham College, Barnard's Inn Hall, Holborn, London EC1N 2HH
Tel: 020 7831 0575 Fax: 020 7831 5208
e-mail: enquiries@gresham.ac.uk