

Feature

Author Jonathan Fisher QC

The UK's faster cheque payment project: a bonanza for cyber-crime fraudsters

The UK has introduced a faster cheque clearance system for the processing of cheques. The change is consequent upon the Cruickshank report which uncovered profound competition problems and inefficiencies in the market for money transmission services. Some of these problems will be only too familiar to bank customers: slow clearing cycles for cheques and automated payments, and high charges for cash withdrawals. As Cruickshank noted, many of these problems can be traced back to the structure of the UK payment systems market which consists of a series of unregulated networks, mostly controlled by a few large banks who in turn dominate the market for services. The key benefit resulting from the change is for customers who accept cheques. For the first time a customer will be certain that after six working days funds cannot be reclaimed as may have happened in the past – typically if the cheque turns out to be fraudulent or if there are insufficient funds in the payer's account.

THE CLEARANCE PROCESS

The current cheque-clearing system is a convoluted process, and as the British Banking Association has pointed out funds are often not available to the customer until the fourth or fifth day. One leading academic text has described the process as cumbersome and suggested that it could be simplified by electronically transmitting an image of the cheque to the drawee bank. When the Treasury Select Committee discussed the problems with cheque clearing, it noted that clearing delays made it hard for retail and business customers to manage their financial affairs effectively which resulted in higher bank charges from unauthorised overdrafts and forgone interest revenues.

Announcing the changes, APACS (the UK trade association for payments) cited

KEY POINTS

- The introduction of one-day cheque clearance in the US heralded an increase in cyber-crime banking fraud and a reduction of the ability of the prosecuting authorities to bring cases to court because of the paucity of documentary evidence.
- The same pattern of activity would be likely to occur if one-day cheque clearance were to be introduced in the UK.
- Banks should lobby for the replacement of cheque banking with biometric fingerprint authorisation of electronic banking transactions as the best way forward.

This article examines the increased exposure to cyber crime which would result if one-day cheque clearance were introduced in the UK.

two key benefits, namely added certainty and increased transparency. APACS noted that for the first time a customer could be certain that after six working days funds could not be reclaimed as may have happened in the past – typically if the cheque turned out to be fraudulent or if there were insufficient funds in the payer's account. There are other practical benefits as well. The change allows customers to take advantage of the shorter cycle as it facilitates the withdrawal of funds earlier than the current time scale, which is particularly onerous for those with limited incomes and small businesses. Further, the shorter clearing process affords some parity with the UK's European counterparts. Belgium, Denmark, Greece, Spain, Finland and the Netherlands all enjoy one-day cheque clearance. In Sweden, the process can take just a couple of hours. Further, the US, South Africa, Namibia and Norway have all implemented one-day clearing processes.

However, the introduction of one-day cheque clearance in the US has not been an unreserved success. As the UK embraces a speedier system for cheque clearance, banks can learn some useful lessons from the US experience, especially as it heralded an increase in cyber-crime banking fraud and a reduction in the ability of the prosecuting authorities to bring cases to court because of the paucity of documentary evidence.

THE US CLEARANCE SYSTEM

Interestingly, the US adopted a one-day clearance system three years ago in order to circumvent the problems articulated in the Cruickshank Report. The key point to note about the introduction of one-day cheque clearance is that it depends upon making greater use of electronic

processing for its efficacy. Whilst the increased application of modern technology is to be encouraged, especially if it confers consumer benefits which would otherwise not be available, ironically it is the greater use of electronic processing which renders the one-day cheque clearance vulnerable to more extensive abuse in the hands of the sophisticated cyber-criminal.

The starting point for a consideration of one-day cheque clearance in the US begins with a consideration of the Federal law passed by Congress entitled Check Clearing for the 21st Century ('Check 21') which came into force on 28 October 2004. The Federal Reserve Board ('FRB') explained that instead of physically moving paper cheques from one bank to another, Check 21 allowed banks to process more cheques electronically. Banks capture a picture of the front and back of the cheque along with the associated payment information and transmit this information electronically. If a receiving bank or its customer requires a paper cheque, the bank can use the electronic picture and payment information to create a paper substitute cheque. This process enables banks to reduce the cost of physically handling and transporting original paper cheques, which can be very expensive.

One of the primary motivations for the introduction of faster, electronic clearing was the impact of 9/11 since it halted all air traffic in the US and as a consequence hundreds of millions of cheques did not move, thus stalling the US payments system. The situation severely undermined economic security and as a result the FRB, after consulting with the banking industry, technology companies and consumer groups, submitted a proposal to Congress that would



reduce the need for physical transportation of cheques through increased electronic truncation.

When it was passed, Check 21 was hailed as solving a long-standing dilemma – how to foster cheque truncation earlier in the cheque collection or return process, without mandating that banks accept cheques in electronic form. The Act facilitates cheque truncation by creating a new negotiable instrument called a substitute cheque which permits banks to truncate the original cheques, to process the cheque information electronically and to deliver substitute cheques to banks that want to continue receiving paper cheques. A substitute cheque, which is the legal equivalent of the original cheque, includes all the information contained on the original cheque – that is, an image of the front and back of the cheque, as well as the machine-readable numbers that appear on the bottom of the cheque.

ENHANCED VULNERABILITY TO FRAUD

The difficulty is that the increased use of electronic applications renders the banking system more vulnerable to fraud. The FRB of Chicago specifically identified fraud as a high risk in implementing the Check 21 Act in terms of forgery, counterfeiting and alteration of original cheques. It identified the risk of duplicate debits due to multiple copies of cheques as a medium threat on the scale, with other risks being the re-crediting provisions in the Act and the poor quality of substitute cheques. Further, as banking sector participants have noted:

‘With more online products like cheque images and statements, banks also can inadvertently provide more information – including signatures – which can help criminals devise fraudulent schemes that do not raise suspicion. Using illegally obtained passwords, sophisticated cyber-thieves can not only access cheque signatures, but also methodically analyse bank statements and customer cheque-writing patterns to plot crimes that bypass most traditional cheque fraud systems.’

(Danielle D’Angelo and Rob Shapiro, Unisys).

Presenting electronic images of cheques is manna from heaven in the hands of fraudsters who have the ability to transfer internet based scams to the one-day processing of cheques. Suppose a spoof email campaign is launched with the purpose of tricking bank customers to disclose their user name and login passwords. Using the fraudulently obtained user names and passwords, the fraudsters then retrieve the customers’ monthly statements and cheque images. Armed with this intelligence, the fraudsters can create high-quality counterfeit cheques that are nearly identical in appearance, drawn for an amount that is appropriate for the account, and bearing a scanned signature. A bank would be hard pressed to detect the fraud before the cheque was processed in a one-day clearance system. What is more, the scale of the problem is potentially enormous. It has been estimated that during 2006 approximately 57 million US adults received ‘phishing’ emails, of which 11 million clicked on the provided links, and 1.78 million provided passwords and other sensitive personal information. In total, the scams resulted in fraudulent losses of \$2.4bn.

To compound matters, there is the additional worry that placing both cheque images and monthly statements online offers fraudsters intelligence on both the visual aspects of the cheques as well as the behavioural history of the account-holder. This type of aggregated intelligence significantly enhances fraudsters’ ability to create counterfeit cheques that circumvent both behaviour-based and image-based detection systems if the customer’s log-in credentials should be compromised. As recent phishing scams indicate, large-scale compromise of customer credentials is a very real possibility.

LOSS OF VALUABLE EVIDENCE

In addition, to compound the vulnerability of the banking sector in this area, the introduction of a one-day cheque clearance system has also made it more difficult in the

US for the prosecuting agencies to bring cases to court because the documentary evidential trail is being compromised. With the Check 21 system contingent on electronic imaging of the cheque, the number of successful prosecutions for fraud has been reduced in the US owing to the fact that the original cheque is not retained after it has been imaged, thereby destroying the fingerprint evidence and the opportunity to analyse writing depressions. As one person in the banking sector explained, ‘if there is fraud, there is no way to check for fingerprints, writing depressions, etc, any evidence of cheque fraud disappears without a trace’.

The problem caused by the lack of documentary evidence in a cheque fraud case was vividly illustrated in the *Wachovia Bank* case (457 F.3d 619 7th Cir. 2006) where, electronic imaging having been employed by the bank, it was impossible to prove that the cheque had been forged. The bank was forced to rely on the argument that since cheque alteration was the classic way of committing fraud in this type of case, in the absence of evidence suggesting to the contrary it was fair to assume that cheque alteration must have occurred in this case. From the perspective of the banking sector, the *Wachovia* case has identified an area of weakness which needs to be addressed as a result of the introduction of the one-day clearance system.

ANTICIPATING THE UK EXPERIENCE

There is no reason to believe that similar problems would not be experienced in the UK if the one-day clearance system were to be adopted in some future endeavour to speed up cheque clearance for the benefit of the consumer. Sophisticated fraudsters would transfer from one country to another if the opportunities for criminality were sufficiently attractive. Having learnt from their experiences in the US, the cyber-criminals could be expected to be at least one step ahead of the UK law enforcement agencies. Long before the introduction of one-day clearance was seriously mooted, APACS in its 2004 Review recognised that there was an expectation that cheque fraud would rise as a result of the Chip and Pin

Feature

Biog box

Jonathan Fisher QC is a leading barrister at 23 Essex Street, London and specialises in fraud, corporate crime and money laundering cases. Email: jonathanfisher@23es.co

programme reducing Card Fraud. APACS also noted that incidents of cheque fraud were increasing substantially in areas of forgery and counterfeit activities, with criminals focusing on identity fraud and improved-quality counterfeiting.

The incidence of Internet scams is equally prevalent on this side of the Atlantic. In October 2004, *The Times* reported that Britain's 14 million Internet bank customers had faced a month of intense bombardment from fraudsters trying to access online accounts in devious phishing scams. Around 60 such frauds, each generating hundreds of thousands of emails, were detected in October 2004. The financial implications for banks were significant since they were not insured against such losses. It was estimated that banks paid out in excess of £4.5m in refunds to approximately 2,000 fraud victims in the first half of 2004. Since then, the growth in phishing scams has been exponential. APACS reported that there were 5,087 cases between January and June 2006 and 7,224 for the same period in 2007.

The extent to which a large-scale compromise of customer account details is possible in the UK was articulated by Ross Anderson, Professor of Security Engineering at Cambridge University who recorded in a paper that during 2006 a single bank sustained £30m of the £35m phishing losses occurring in that year. Professor Anderson described the development of a growing underground economy indicative of the level of sophistication of such frauds. What is more, the frauds were committed in increasingly sophisticated and international ways.

UK CASES

In point of fact, a number of serious cyber-crime fraud cases have already occurred in the UK. The first reported conviction in the UK for a phishing scam was that involving David Levi, who was convicted of fraud at Preston Crown Court in 2005. He obtained £200,000 by harvesting online auction account details and bank details. Levi was sentenced to a term of three years' imprisonment for fraud and 12 months for perverting the course of justice for targeting Ebay customers and persuading

them to disclose their bank account details. *The Daily Telegraph* reported that Levi and his gang sent emails purporting to come from the auction site itself. Those who replied on a quick link were connected to the gang's computer network, allowing the fraudsters to assume their cyber identities. The fraudsters then advertised high-value items for sale and took the proceeds of such sales. The scale of the fraud was that over 160 people were duped in the course of one year, between July 2003 and July 2004.

A slightly earlier case in Leeds involving Douglas Havard and Lee Elwood in June 2005 was more directly related to banking fraud. The defendants were convicted of conspiracy to defraud and launder money, with Havard and Elwood receiving imprisonment terms of six years and four years respectively. This phishing scam involved obtaining information about the victim's identities and their bank account details which were then used to access money from cash machines and buy and sell goods online. When Elwood and Havard were arrested, forged bank documents, forged traveller's cheques, computers and forged holograms were seized.

CONCLUSION

If UK banks are to avoid exposure to significant fraud losses perpetrated by sophisticated cyber-criminals similar to those sustained by banks in the US, UK banks should resist any attempt to import the one-day cheque clearance and instead lobby for the replacement of cheque banking with biometric fingerprint authorisation of electronic banking transactions as the best way forward. There have already been moves by banks in the US to utilise advances in biometric technology to enhance security, and if developments in the US are to be replicated in the UK, the introduction of a biometric technology is a better model. Biometrics UK report that 12 branches of Zions Banks in Utah and Idaho have recently implemented biometric fingerprint technology for cashing cheques. Moreover, a group of academics based at the University of Tennessee have also suggested a biometric identification method which utilised

electronic signature equipment which would work by sensing the pressure, pattern and speed of the electronic pen and verifying this signature against authenticated signature information which would allow forgeries to be detected.

Looking to the future, there are clear indications that cheque banking is coming to an end, especially as the Chip and Pin system for plastic cards has been hailed as a significant success. A representative from Visa has expressed the view that cheques are fast becoming an obsolete method of payment as the cost to retailers of fraud, processing and queuing is recognised. High-street retailers such as Boots, PC World, Currys and Next have announced that they will no longer accept cheques as a method of payment and the declining use of cheques in the retail sector is indicative of their reduced significance more generally in the banking sector. Further, APACS has produced forecasts which suggest that cheque use as a whole may be coming to an end, predicting that by 2015, cheques will account for under 1 per cent of all retail transactions and that one in 20 invoices will be paid by cheque.

Ultimately, therefore, the vulnerability of the banking sector to fraudulent activity will spell the end of cheque banking, with biometric fingerprint authorisation of banking transactions as the way forward. Since the costs of fraud are unavoidably passed down to the customer, it is regrettable that the introduction of one-day clearance in the US, which was promoted as a consumer protection measure, has had such unfortunate consequences. The banking sector must be vigilant to ensure that the dismal US experience is not replicated in the UK, whilst at the same time promoting an efficacious alternative system which would afford the consumer an opportunity of 'real-time' banking, combined with the advantage of security. ■

This is an extract of a paper given at the 25th International Symposium on Economic Crime held at Jesus College, University of Cambridge, on 6 September 2007. The full version is published in the *Journal of Financial Crime*, March 2008 edition.