Citadel Advantage

CA Digest

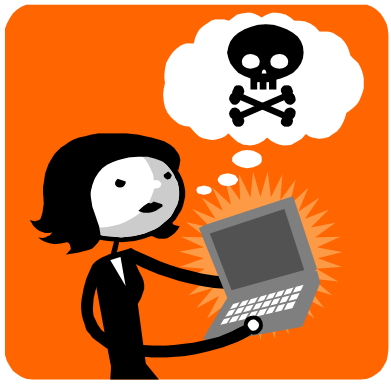
PAYMENTS NEWS YOU CAN USE

Biweekly Digest of Payments & Related Information from the around the World

No: 139 **Date: 13th February 2008**

In Focus

McAfee says Web attacks are top global security threat



Attacks targeted at Web-based services will constitute one of the 10 biggest global security threats in 2008, warns McAfee in its latest Virtual Criminology Report. The Internet security firm compiled the study with the aid of agencies such as the FBI.

The study paints an alarming picture of cyber criminals taking control of thousands of Internet-connected computers to attack Web banking services, payments networks, financial markets, government databases and even electricity systems

"We are in a virtual arms race," says Dave DeWalt, McAfee's CEO and president. "Fighting cyber crime is a 24/7 and global battle."

DeWalt says the fight against cyber crime involves action at all levels, from private individuals upwards. "Whether it be organizations securing their networks, or governments writing enforceable legislation to deter criminal behavior, we must work together to stay ahead," he says.

According to the study, topping the list of global threats affecting individual Internet users in 2008 will be attacks using sophisticated new software. An example is Storm Worm, a malware program which gives cyber criminals full control over a large number of users' PCs.

Another type of threat targets new technologies such as peer-to-peer networks and voice over Internet Protocol (VoIP) services. An additional category of attack targets online social networks such as MySpace and Facebook. These sites are used by cyber criminals to mine personal information, trick users through phishing scams, and serve up malware.

"Who needs to 'dumpster dive,' when all a fraudster needs to do is log on to a social networking site?" says Lilian Edwards, a researcher at the Institute for Law and the Web in Southampton, UK.

While direct losses to Internet users via privacy breaches may be small, McAfee fears the cumulative effect could be the erosion of trust in online businesses and in public institutions such as banks and government agencies.

Risk Management Tips

Citadel Advantage puts you in control when managing Operational Risk

Contractual Arrangements

Is your bank a participant in a shared EFT/POS network or does it contract with a third-party card-issuing or -acquiring processing service provider/s?

If either of these scenarios fit your bank have you checked that;

- Contracts with local/regional EFT/POS network switch and gateway operators and card processors clearly set forth the rights and responsibilities of all parties, including the integrity and confidentiality of customer information, ownership of data, settlement terms, contingency and business recovery plans, and requirements for installing and servicing equipment and software?
- Adequate agreements are in place with all vendors supplying services for retail EFT/POS and card operations (plastic cards, ATM equipment and software maintenance, ATM cash replenishment) that clearly define the responsibilities of both the vendor and the bank?
- Agreements include a provision of minimum acceptable control standards, the ability of the bank to audit the vendors operations, periodic submission of financial statements to the bank, and contingency and business recovery plans?
- Contracts and agreements clearly define responsibilities and limits of liability for both the customer and bank and include provisions of any related legislation or legally binding rules?

Does management periodically reviews individual sites providing retail EFT/POS and card services to ensure policies, procedures, security measures, and equipment maintenance requirements are appropriate?

In the case of retail EFT/POS and card transaction processing activities contracted to third-party service providers, does management assess the adequacy of the review process performed by management regarding annual financial statements and audit reports?

Special Report

SEPA – What SEPA?

Just a hiccup? Judge for yourself….

David Birch writing in the Digital Money Forum Blog on 6 February said;

"Unlike many of you, I am very fortunate to have access to a) a euro bank account and b) someone that I can ask to waste their time on payment-related lunacy. Put these two things together and a SEPA experiment was born: I decided to celebrate the birth of the SEPA zone and send some euros to one of our Forum friends in the Netherlands, thus becoming (I hope) the first blogger to originate a SEPA Credit Transfer (SCT).

Well, my plan fell at the first hurdle because according to our bank (who shall not be named in this piece, but it's one of the U.K.'s big four) "SEPA transfers are not available online". Yes, that' s right. Gertrude's (Gertrude Tumpel-Gugerell - Member of the Executive Board, European Central Bank - Editor) *dream of a friction-free payments landscape was in tatters, and it was only day 1. Someone had to physically go to the bank in order to do a SEPA Credit Transfer.*

Most normal consumers would, of course, have given up at this point and forgotten about the whole SEPA thing. But I'm not a normal consumer. I have a responsibility to Digital Money Denizens and will leave no stone unturned, no path untravelled in order to send some euros to Amsterdam. So I sent someone down to the bank (not because I was lazy, but because I was out of the country).

She came back with a paper form to fill out. This was done, and the form was returned to the bank on a Tuesday, and on Friday I received confirmation from my Dutch colleague that the money had arrived in this account,

So, in summary, sending 50 euros to Amsterdam in the exciting new world of SEPA took two trips to the bank, cost £15 (i.e., a transaction fee of 40%) and took three days. Next time, I'll use PayPal."

Comments anyone?

(E-mails to CADIGEST@citadeladvantage.com with "Comments" in the Subject line)

Biweekly Digest of Payments & Related Information from the around the World

UPCOMING CITADEL ADVANTAGE TRAINING COURSES

NEWLY added items are highlighted in BLUE

Please click on the ***Details*** box for full course details

All our Payments & Risk Courses have been updated to include details of the US Sub-Prime crisis and its affects on Payments Systems Liquidity & Risk Management

All Risk Courses include a SocGen Case Study

25 - 26 February 2008	REMITTANCES - CREATING VALUE	Johannesburg	Citadel Advantage	***Details***
28 -28 February 2008	REDUCING RISK IN FOREIGN EXCHANGE SETTLEMENT	Johannesburg	Citadel Advantage	***Details***
10 - 12 March 2008	BUSINESS CONTINUITY & SCENARIO PLANNING FOR BANKS	Singapore	In conjunction with Ethan Hathaway	***Details***
31 March - 1 April 2008	DOMESTIC PAYMENTS	London	In conjunction with Marcus Evans	Details coming soon
7 – 8 April 2008	MANAGING RISK IN RETAIL PAYMENT SYSTEMS	Gaborone, Botswana	In conjunction with Logitech	Details coming soon
9 – 10 April 2008	MANAGING RISK IN ELECTRONIC BANKING: TAMING THE ELECTRONIC TIGER	Gaborone, Botswana	In conjunction with Logitech	Details coming soon
5 - 6 May 2008	PAYMENTS AMERICA	New York	In conjunction with Marcus Evans	Details coming soon
12, 13 & 14 May 2008	**OPERATIONS RISK MANAGEMENT – BEYOND COMPLIANCE – A VALUE ADDED APPROACH**	**Johannesburg**	Citadel Advantage	For details see last page of CA DIGEST
19 - 20 May 2008	INTERNATIONAL PAYMENTS	London	In conjunction with Marcus Evans	Details coming soon
16 - 18 June 2008	BUSINESS CONTINUITY & SCENARIO PLANNING FOR BANKS	Dubai	In conjunction with Ethan Hathaway	***Details***
17 – 18 July 2008	**INTERNATIONAL PAYMENTS**	**New York**	**In conjunction with Marcus Evans**	Details coming soon
5 - 6 August 2008	MANAGING RISK IN ELECTRONIC BANKING: TAMING THE ELECTRONIC TIGER	Hong Kong	In conjunction with Ethan Hathaway	***Details***
7 - 8 August 2008	REDUCING RISK IN FOREIGN EXCHANGE SETTLEMENT	Hong Kong	In conjunction with Ethan Hathaway	***Details***
24 - 26 September 2008	BUSINESS CONTINUITY & SCENARIO PLANNING FOR BANKS	Hong Kong	In conjunction with Ethan Hathaway	***Details***
20 – 21 November 2008	PAYMENTS AMERICA	New York	In conjunction with Marcus Evans	Details coming soon

Operations Risk

Canada

Huge credit card fraud detected

Two Canadian women have been charged with fraud after Police in Edmonton, Alberta found 30,000 files containing stolen credit card numbers on a home PC. The women, Elena Banfield and Stacey McGillis, face over 30 fraud-related charges.

The investigation began on January 9, when a traffic policeman pulled over Banfield's car in Edmonton for a motoring offense, and she gave him a false identity document. Banfield also had several stolen credit cards in her possession in the car. The police then searched the house shared by Banfield and McGillis. The search revealed the credit card data files, as well as around 500 stolen identity documents such as passports, birth certificates and provincial healthcare cards.

According to press reports, most of the stolen items had been taken from mailboxes in the neighborhood where the 26-year-old women rented a house.

The Edmonton Police Department says it will take officers months to go through the list of people whose names and credit card numbers were stored on computer, and then contact the victims.

France

Government report alleges risk and security failures at SocGen

A probe into the EUR5bn Société Générale rogue trading scandal by the French government has revealed that the bank was warned last year that its security systems and internal controls were lacking.

French Finance Minister Christine Lagarde told reporters that SocGen failed to apply appropriate controls over Jérome Kerviel, who was allegedly able to use loopholes in controls and circumvent risk management procedures to make a series of unauthorised bets on European futures.

Kerviel's deals eventually led the bank to reporting €4.9 billion in losses last month. It is thought that Kerviel's trades exceeded the bank's market value.

Lagarde's report states that inspections by the banking commission carried out in 2006-7 had led to recommendations that SocGen "strengthen the security of operations".

Lagarde told reporters that SocGen missed a number of "alarms", most notably in November when derivatives exchange Eurex alerted the French bank about the positions in Kerviel's book.

Although the report backs up SocGen's version of events, Lagarde has called on banks to reinforce "Chinese Walls" between the back, middle and front office and to monitor unusual behaviour - such as when a trader does not take holidays.

Reports emerged last week that Kerviel only took four days of holiday in 2007.

In a statement SocGen claims Lagarde's report "does not call into question the systems used to manage market risk".

"Concerning the controls which were successfully circumvented by the fraud, the

measures which would have enabled its detection and prevention have already been implemented or will be put into place shortly," says the bank.

International

Phishers targeting phishers

In a new twist, would-be fraudsters are being scammed by a gang offering free do-it-yourself phishing kits on the Internet, says e-security firm Netcraft.

The kits are the work of a group of Moroccan fraudsters known as "Mr. Brain", says Netcraft's Paul Mutton in a blog. Hidden code embedded in the kits sends any personal information stolen by would-be fraudsters back to Mr. Brain.

The gang has launched a Web site offering kits for targets such as Bank of America, eBay, PayPal and HSBC. On offer to potential fraudsters are phishing site code, e-mail templates and other hacking tools. Mutton says the tools and code make it easy and quick for fraudsters to set up phishing sites with only a basic knowledge of PHP programming.

NetCraft says the gang's site claims the kits can be used to steal confidential data such as social security, credit card and PIN numbers. The gang claims the kits are undetectable by Mozilla, Opera and Internet Explorer browsers.

But, what the kits' users don't know is that hidden code sends the stolen details back to the Mr. Brain group's e-mail accounts. Mr. Brain disguises its e-mail address by exploiting the case-sensitivity in PHP variable names.

"Most fraudsters are unlikely to notice this level of obfuscation and will assume the script is working normally, as they will also receive a copy of any e-mails produced by the script," says Mutton in his blog.

"Such deception is a useful tactic for any fraudster who wishes to maximize the number of successful attacks, as the work of deploying the phishing sites and sending the mails is then carried out free of charge by novice fraudsters on behalf of the author," adds Mutton.

Earlier this month Mutton says he warned of a similar scam involving a kit that targets Bank of America customers.

Singapore

Ex-Citi bankers charged under Singapore's Computer Misuse Act

Seven former Citibank staff are facing over 1000 charges under Singapore's Computer Misuse Act and bank secrecy laws over client details allegedly stolen from the US bank and passed on to rival firm UBS.

According to reports, the group of private bankers face a total of 1,223 charges for allegedly accessing Citibank's computer network without authority and downloading or printing client data. The data was taken before all seven left Citi to join rival bank UBS in 2006.

A police spokeswoman told local media the charges could carry fines of over S$125,000 and up to 20 years in prison.

The charges were filed after Singapore police completed a year-long investigation into the incident. The police investigation began after Citibank filed a lawsuit against six of the accused in 2006. The lawsuit was settled out of court last year.

It is thought this is the first case where Singapore authorities have used the Computer Misuse Act and banking laws to prosecute the theft of customer information. The group have been granted bail ahead of a pre-trial session.

Sweden

Bank foils hackers

A gang of Swedish hackers was seconds away from completing a digital bank robbery last summer when an alert bank employee literally pulled the plug on their scam.

The would-be bank robbers had placed "advanced technical equipment" under the employee's desk that allowed them to take control of his computer remotely, Swedish prosecutor Thomas Balter Nordenman said in a statement. Nordenman declined to name either the employee or the bank he works for.

The employee discovered the device shortly after he realized his computer had started an operation to transfer a significant amount of money from the bank to another account. "By pulling out the cable to the device, the employee managed to stop the intended transfer at the last second," Nordenman said.

The attempted theft happened in August 2007 at a bank in Uppland County, north of Stockholm, police said. They announced it on January 30, 2008 after seven suspects, all from the Stockholm region, were arrested while allegedly preparing another heist.

Police did not name the suspects, but said many of them have prior fraud and theft convictions. Investigators did not give other details on the device, or how it was placed under the desk.

Japan

Systems glitch hits Tokyo Stock Exchange

The Tokyo Stock Exchange (TSE) was forced to suspend trading last week in a key futures contract after its recently-installed derivatives trading platform was hit by a systems glitch.

According to press reports, the glitch forced TSE to halt trading in March futures contracts for the Topix index just before the close of morning trading. Trade remained halted throughout the afternoon, preventing traders from closing positions in the contract.

The derivatives system, which was developed by Fujitsu, went live last month following delays. Fujitsu is also working on a new trading platform to be rolled out by the TSE next year.

This latest incident has raised new concerns about the trading infrastructure at the TSE, which suffered a series of embarrassing and costly operational failures in late 2005 and 2006 which cost TSE president Takuo Tsurushima his job.

In November 2005 the TSE suffered a systems crash that halted trading for more than four hours, which was later blamed on Fujitsu. Just two week's later the TSE's computer systems failed to cancel a mistaken order from a fat-fingered Mizuho trader to sell 610,000 shares for one yen, instead of one share for Y610,000. Furthermore in January 2006 the Tokyo exchange was forced to close trading early after its system was unable to cope with a surge in sell orders.

Following these incidents TSE said in 2006 that it was investing around US$529 million on overhauling its Fujitsu-built trading technology. But after inviting financial technology vendors to tender for the contract to overhaul the technology, the TSE eventually awarded the deal to Fujitsu.

United Kingdom

Laptop with personal data stolen

UK's Ministry of Defense (MoD) has reported that a laptop containing the personal information of 600,000 people has been stolen recently from a Royal Navy officer.

The MoD says it is writing to around 3,500 people whose bank account details were on the laptop. Payments association APACS is helping

to inform banks so that accounts can be monitored.

Other information on the computer includes national insurance numbers and passport details.

The MoD says the information held is not the same for every individual. In some cases the record is no more than a name. But for other "extensive personal data" may be held, including passport details, National Insurance numbers, drivers' license details, family details, doctors' addresses and National Health Service numbers.

FSA fines Norwich Union Life £1.26m for loose security

The UK's Financial Services Authority (FSA) has fined insurer Norwich Union £1.26 million for failing to protect confidential customer data - including bank account information - from fraudsters.

The City watchdog says Norwich Union's life assurance unit did not have effective systems and controls in place to protect customers' confidential information and manage financial crime risks. These failings resulted in a number of actual and attempted frauds against policyholders.

Slack call centre security allowed fraudsters to use publicly available information - including names and dates of birth - to impersonate customers and obtain sensitive customer data, says the FSA. In some cases criminals were able to ask for confidential customer records, such as addresses and bank account details, to be altered.

The fraudsters then used the information gleaned to request the surrender of 74 customers' policies totaling £3.3 million in 2006.

The FSA says its investigation found that Norwich Union Life failed to properly assess the risks posed by financial crime and as a result, its customers were more likely to fall victim to identity theft.

Furthermore, the insurer failed to address the issues properly, even when it had been alerted to the problem by its own compliance department.

"Norwich Union Life let down its customers by not taking reasonable steps to keep their personal and financial information safe and secure," says Margaret Cole, director of enforcement, FSA. "It is vital that firms have robust systems and controls in place to make sure that customers' details do not fall into the wrong hands. Firms must also frequently review their controls to tackle the growing threat of identity theft."

In a statement, Mark Hodges, chief executive of Norwich Union Life, says: "We have extensive procedures in place to protect our customers but in this instance weaknesses were exploited and we were the target of organized fraud."

"Whilst the number of customers affected is very small compared to the number of policies we manage overall, any breach in customer confidentiality is clearly unacceptable," he adds.

Hodges says the firm has "thoroughly reviewed" systems and controls following the FSA's investigation.

Norwich Union Life is the latest in a number of financial service providers that the FSA has fined for failing to protect confidential customer data. In the past two years the watchdog has slapped fines BNPP Private bank, Capita Financial Administrators and Nationwide Building Society for failings relating to information security lapses and fraud.

Details of the latest fine comes as UK Chancellor prepares to face questions from MPs about the loss of personal data on 25 million child benefit claimants was lost by HM Revenue and Customs (HMRC) last month. Darling will outline the preliminary findings of a review into the security breach.

Halifax facing chip and PIN fraud lawsuit

High street bank Halifax is facing a lawsuit brought by a customer who claims that fraudsters cloned his chip-based card and withdrew £2,100 from his account at ATMs.

Alain Job said that he changed the PIN supplied by the bank to a number that only he knew and was in possession of his card when fraudsters raided his bank account.

But the Halifax claims that whoever took the money had access to both Job's card and PIN. Job is in the process of bringing his case against the Halifax to court.

The case casts further doubts over the effectiveness of chip and PIN which was introduced in the UK two years ago in order to eliminate skimming scams where fraudsters copied data stored on the magnetic stripe of a credit to make cloned cards.

Although chip and PIN contributed to a drop in domestic fraud levels fraudsters have switched to using cloned cards abroad in places where chip and PIN hasn't yet been implemented.

A security expert, Mike Bond, said that as well as mag-stripe cards chip-based cards can be copied and cloned, although the technique is more cumbersome and expensive as it involves stealing the PIN and copying a secret key stored on the chip which is used by banks to validate cards. Bond says that, whilst it is possible that criminals have found a cheaper way to extract data from the chip, there is no evidence that this has happened.

A cheaper way for fraudsters to clone cards is to create a "yes card", says Bond, which doesn't contain a copy of the original card's PIN and secret key.

Instead, the fraudster copies the rest of the chip's data to a smart card. This "yes card" will work with chip-and-pin implementations using a security technique called Static Data Authentication (SDA), says Bond, which enables chip readers to authenticate a transaction without directly contacting a bank.

However, this technique does not explain Job's losses because all ATMs contact banks for authentication, says the report.

United States

FBI says VoIP "Vishing" scams Increasing

Telephone phishing attacks against US banks and consumers continue to rise at an alarming rate, warns the FBI. These so-called vishing attacks are facilitated by the use of voice-over-IP (VoIP) technology, which allows criminals to make cheap and anonymous calls to intended victims.

Vishing operates like phishing, by using automated voice recordings or emails to persuade consumers to make a call and divulge their Personally Identifiable Information).

In their vishing messages, criminals claim customer bank accounts are suspended, deactivated, or terminated. They then provide a telephone number and ask recipients to contact their bank. This, of course, is not an authentic bank telephone number.

People who call the "customer service" number are greeted with a message supposedly from their bank. They are then led through a series of voice-prompted menus that ask for account numbers, passwords, and other critical information in order to resolve a "pending" security issue.

The whole operation is facilitated by the use of VoIP, says the FBI. Because of the low cost of long-distance VoIP calls, the scam is cheap for criminals to set up. And, because VoIP is Web-based, criminals can use software programs to create phony automated customer service lines.

VoIP calls are not always easy to trace, says the FBI. This is because criminals thwart caller ID systems by masking the number they are calling

from, while in other cases they hack into the VoIP service of a legitimate subscriber and use it to defraud people.

GE Money reports customer data loss

Card issuer GE Money has reported that a computer tape containing confidential information belonging to over 650,000 credit card holders has been lost.

According to press reports the back-up computer tape was being held by data storage firm Iron Mountain. The firm told GE Money that the tape was missing from its warehouse in October.

The tape is thought to contain credit card information for customers of around 230 retailers, including JC Penney. Reports say the tape also includes the social security details of around 150,000 people.

GE Money is reportedly writing to those affected by the data loss and says it will pay for 12 months of credit monitoring for customers whose social security numbers were lost.

The disclosure comes a year after US retailer TJX reported a security breach that resulted in the theft of millions of credit card numbers.

Hackers placed unauthorized software on TJX's computer network and stole at least 100 files containing data on millions of accounts. Debit and credit card data exposed in the breach is thought to have been used to make fraudulent purchases in Florida, Georgia and Louisiana in the US, as well as in Hong Kong and Sweden.

Phishers targeting corporate treasury accounts

The Anti-Phishing Working Group (APWG) says phishers are increasingly targeting corporate treasury staff in order to raid company bank accounts. The US-based security organization also says that the number of individual brands hijacked by phishers in November 2007 exceeded all previous records.

In November last year, 178 financial institutions and government agencies such as tax offices had their identities co-opted by fraudsters for phishing campaigns.

"We are seeing executives of companies receiving specially targeted emails that attempt to do two things," says Laura Mather, managing director of operational policy for APWG,. "Firstly, install malware to give the phisher access to the corporations' systems, and secondly gain access to the corporations' bank accounts."

Bank spending on compliance soars – Deloitte

The latest research from Deloitte shows that expenditure on compliance by US banks has increased an average of 159% over the past five years, but the majority of spending - 60% - goes on staff costs while only 18% is dedicated to technology.

Deloitte says its survey of 20 banking and thrift institutions in the US found that spending on compliance has increased drastically in recent years, and is likely to increase further in light of the recent focus on mortgage lending practices.

But the majority of direct compliance spending went to compensate staff, according to respondents, while only 18% went to capital expenses, mainly IT systems, hardware and software.

Don Ogilvie, the independent chairman of the Deloitte Center for Banking Solutions, says the tendency has been to respond to increased regulations by adding people, rather than by leveraging technology and improving processes,

The way banks have chosen to manage compliance may have added to costs, says Ogilvie.

"It is clear that banks could mitigate rising compliance costs by putting more focus on a new approach to compliance management, one that reduces duplicative - and redundant - processes and builds business cases for more investment in technology solutions," he adds.

However Deloitte says some respondents estimated their institution's IT spending was 10% to 15% higher than it would have been without additional compliance requirements. They noted IT systems designed for monitoring, controls and regulatory policies experienced the most rapid increases in capital investment.

Respondents also reported that IT initiatives designed to drive increased revenue or upgrade risk management had been delayed over the past three years, due to the priority placed on compliance-related projects.

Only five per cent of respondents said increased compliance had led to reduced functional duplication, and 30% of those surveyed claim that duplication had actually increased.

In addition, as many as 95% of respondents said management and administrative employees at their institution were spending more time on compliance than before.

Did You Know?

Antivirus software	Computer programs that offer protection from viruses by making additional checks of the integrity of the operating system and electronic files. Also known as virus protection software.
Applet	A small program that typically is transmitted with a Web page.
Application	Either a software program designed for use by end users or software that performs automated functions for a user. Examples include home banking, word processing, and payroll. Distinguished from operating system or utility software.
Application controls	Controls related to transactions and data within application systems. Application controls ensure the completeness and accuracy of the records and the validity of the entries made resulting from both programmed processing and manual data entry. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.

With each edition of the CA DIGEST we bring you a free Operations / Risk Management information.

Payment, Settlement & Banking Systems

Australia

ANZ pilots mobile banking

ANZ Bank is piloting a new full-service mobile banking service with customers in Australia ahead of a public launch later in the year. Internet and phone banking customers can use their existing password to register for the pilot m-banking service via a promotion on the ANZ Web site.

The bank says the full Java version of its service will enable customers to use their hand sets to transfer funds between accounts as well as send money to other people.

Users can also check balances and view mini statements showing the last 10 transactions. A text banking option enables users to check account balances, view mini statements and receive account alerts.

The bank says its mobile banking service is free during the trial but says it fees and charges may be introduced with the public release.

ANZ, which already operates a similar m-banking service in New Zealand, is thought to be the first major Australian bank to launch a full mobile banking offering. Rival banks NAB and CBA have both focused on contactless mobile phone payments, running pilots last year.

India

ICICI Bank introduces mobile banking application

India's ICICI Bank has launched iMobile, a mobile banking platform that enables customers to use their handsets to transfer funds and pay bills.

The bank says the free tool enables customers to transfer funds from ICICI savings, demat, credit card and loan accounts using their mobile phones. Money can be sent to ICICI accounts as well as those held with other institutions.

Customers can also use their handsets to pay utility bills and insurance premiums.

Customers who are registered for mobile alerts from the bank can download the application by sending an SMS. Those that have a GPRS connection will then receive a WAP link for activation. Customers without GPRS can download the application from the bank's Web site on their desktop before transferring it to their handset.

The bank says that to ensure security users will need to enter a four digit PIN to use iMobile.

"With this application, most features of Internet banking will now be available on mobile phones, providing a breakthrough improvement in banking services," says V Vaidyanathan, executive director, ICICI Bank.

Last year India topped a survey on mobile banking penetration in Asia Pacific conducted on behalf of Sybase 365. The poll found that 81% of respondents were aware that they can check their bank balance on a mobile phone and 49% had used the services in the previous three months.

United Kingdom

London drivers use mobiles for parking payments

Paying for parking in the UK has just got futuristic with the introduction of "pay by phone" technology in the London district of Southwark.

The system allows drivers to pay for their parking and top up their parking time by using their debit or credit card over a mobile phone. It even sends a text message reminder to the driver's mobile phone when the parking time is due to expire.

Once registered, drivers will be able to pay for their parking in as little as 30 seconds over a mobile phone. Drivers will still be able to pay by coin if they wish. The pilot scheme is currently available in three of Southwark's controlled parking zones. If the 18-month pilot proves popular and successful, it will be made available throughout Southwark.

Southwark Council has teamed up with the pay-by-phone company RingGo which is providing the technology and support for the pilot. Drivers registered will be able to pay by phone in other towns around the UK which have also teamed up with RingGo. Parking attendants will be equipped with a special mobile phone that will show them which cars in the street have paid for parking by phone.

Payphone-ATM use blocked by local town

Telco BT's plan to roll out hybrid payphone-ATMs across the UK has encountered an unexpected obstacle in the seaside town of Skegness. Local councilors said the location of a proposed BT payphone-ATM might make users vulnerable to 'shoulder-surfing.'

The town council's planning committee has recommended that an application by BT Payphones to convert a public telephone to a payphone-ATM be blocked.

BT Payphones wanted to site its payphone-ATM outside a clothes store in Skegness. But councilors said people shopping in the store might be able to see a cardholder entering their PIN into the ATM through the shop window.

Last year, an application by Cardpoint, an independent ATM operator, to install an ATM outside another Skegness store was turned down on safety grounds.

BT is working with financial institutions such as HSBC, Barclays Bank and Nationwide Building Society as well as with independent ATM operators to roll out payphone-ATMs across the UK.

United States

Alternative payments growing rapidly

Alternative payment methods (APM) such as PayPal, Bill Me Later and Google Checkout grew significantly in 2007 and are now offered by 30 percent of the top 100 US online retailers. Between February and November 2007, the number of top online US retailers offering some form of APM grew by 25 percent, says interactive marketing firm Brulant.

By November 2007, Bill Me Later was offered by 21 percent of top online retailers, PayPal by 19 percent and Google Checkout by 20 percent. The adoption rates in February 2007 had been 17 percent for Bill Me Later, 6 percent for PayPal and 5 percent for Google Checkout.

US retailers offering all three forms of APM grew from zero percent in February 2007 to 5 percent in November 2007, according to Brulant. Toys "R" Us, PetSmart and Rite Aid each now offer all three payment methods, Google Checkout, PayPal and Bill Me Later.

The growth of retailers offering all three forms of APM is one of the most surprising findings of the survey, says Adam Cohen, a Principal with Brulant. "This adoption reinforces the 'customer is king' mentality, as retailers begin to offer a multitude of choices for checkout," says Cohen.

Increasing customer satisfaction and driving sales is the reason why US bookseller Border plans to offer alternative payment methods on its new Borders.com site which will be launched in the first quarter of 2008. "We believe these options will help increase customer satisfaction

and potentially drive sales," says Kevin Ertell, Vice President of e-business for Borders.

PayPal to acquire online risk outfit Fraud Sciences

Person-to-person payments operation PayPal is acquiring Fraud Sciences, an Israel-based developer of online risk tools, for $169 million. In a statement PayPal says Fraud Sciences' risk technology will enhance its own proprietary fraud management systems and those operated by its parent company eBay.

"Integrating Fraud Sciences' risk tools with PayPal's sophisticated fraud management system should allow us to be even more effective in protecting eBay and PayPal's hundreds of millions of customers around the world," says Scott Thompson, president of PayPal.

The online auction house says the acquisition of Fraud Sciences fits its plans to "significantly improve trust and safety across its sites in 2008".

Key personnel from Fraud Sciences, including COO Yossi Barak and founders Shvat Shaked and Saar Wilf, will join PayPal's technology and fraud management teams. The acquisition, which is subject to conditions, is expected to close within the next 30 days.

In a separate move, PayPal has signed up to the Iconix Truemark service, which will be available to all its account holders. By placing an icon next to legitimate e-mail messages, the Iconix Truemark service helps consumers visually identify legitimate e-mail messages and avoid phishing attacks. The system uses industry-standard technologies such as DKIM, Domain Keys, SPF and SenderID to verify the authenticity of messages. The application then takes the process a step further by checking the identification of the e-mail sender against a list of registered senders with Iconix. Once an e-mail has passed Authentication and Identification steps, a Truemark Check-lock icon is displayed in the consumer's inbox.

In addition to PayPal, the Iconix service identifies legitimate e-mail messages from nearly 500 other companies, including eBay.

"While there remains no silver bullet solution for protecting consumers against phishing, we continue to explore new technologies to help our consumers stay safer online," says Mike Vergara, director of account protections at PayPal. "Our customers have told us that tools like Iconix help them easily identify legitimate PayPal email, reducing their risk of falling for phishing attacks."

PayPal and eBay are still the brands most spoofed by phishing fraudsters, according to research released by Gartner in December.

Zimbabwe

RTGS failure hits banks

The Bank of Zimbabwe's Real Time Gross Settlement system, which is based in South Africa, has been experiencing operational problems due to connectivity failures on the Masvingo and Beitbridge telecom lines.

Zimbabwe banks use the RTGS system operated by the Reserve Bank of Zimbabwe, which transmits to the systems server located in South Africa. The South Africa server mirrors the transaction through to Belgium and then back to South Africa.

The main problem with the system is that when the transactions are being relayed back to Zimbabwe they depend on electricity to power up the antennas at Beitbridge on the South African _ Zimbabwe border.

TelOne says that the spate of the prolonged recent power cuts had caused the failure and the link station at some point had run out of diesel. TelOne acting managing director Mr Hampton Mhlanga said that they were hopeful that the situation would get back to normal soon.

He said that the generators at the station, which houses the antenna "gobble up a lot of diesel". That in itself was an expensive drawback.

As a result of the system failure, most Zimbabwe workers have not accessed January salaries although some banks with serious liquidity problems could be using the breakdown as an excuse. Stock broking firms have been the worst affected as they are not required to accept cash. A large portion of RTGS transactions is related to the settlement of financial market transactions.

Banks have suggested a temporary switch to manual money transfer and have therefore called for an urgent review in the cheque limit to Zim$20 billion as a way of solving the RTGS backlog.

"If RTGS transactions can start above Zim$20 billion then the delays can be solved," said a bank executive adding that business should start accepting cheques since they were faster and provided auditing details.

Reserve Bank of Zimbabwe Governor Dr Gideon Gono without giving a specific date said that the cheque limit, which is currently at Zam$500 million, would be reviewed soon.

Ultimately, however the goal should be to localize the transfer system as the current failures could affect financial system stability as a whole.

Zimbabwe has been experiencing difficulties in its real time system for over a month.

Basel II

European Union

EU Basel II update will include reactions to liquidity crisis

EU internal market and services commissioner Charlie McCreevy has confirmed that amendments to Basel II will be issued no later than October this year.

Taking into account the lessons learned from Northern Rock and the current volatile market conditions, the amendments will cover issues including liquidity risks, risks from large exposures and strengthening the requirement to provide information to supervisors of a bank's branches, says David Wright, deputy director general of the European Commission's internal market division.

The Commission's announcement comes on the heels of the latest round of Basel II bashing in the press, which has increased since the UK House of Commons Treasury Committee published its report on the run on Northern Rock.

Industry commentators are questioning the effectiveness of Basel II capital requirements, because it appears that issues surrounding liquidity, not capital, caused the run Northern Rock, the first on a bank in a decade. The liquidity issue was related the US sub-prime crisis. The amendments intend to look into this issue, which was omitted when the original Basel II Accord was conceived.

Committee for European Banking Supervisors reports on Pillar 3 implementation

The Committee for European Banking Supervisors (CEBS) recently published the results of its survey on the EU's implementation of the New Basel Accord's Pillar 3 regulation. This survey, of CEBS members, took place late last year and the results were discussed at a workshop of European financial industry participants on December 7th. A summary of the discussions at this workshop was also released.

The overall message from the CEBS is "not to worry" and that the implementation of the Pillar 3 provisions does not give rise to major concerns. This is reported as being mainly due to supervisors and regulators not making prescriptive statements – the principles-based approach. The report says that there are a small number of areas that need further attention and proposes follow-up work in particular to the application of the disclosure requirements to (significant) subsidiaries and to devising a possible solution where limited disclosure is being provided with a subsidiary's (individual) financial statements. Also open is the relationship between Pillar 3 and accounting disclosures; here CEBS will wait on the outcome of industry initiatives before deciding what to recommend.

The follow-up industry workshop was supportive of the CEBS findings. It focused on three areas - disclosures of significant subsidiaries, the content of the current Pillar 3 disclosures (including disclosures in the current market situation), and education of market participants and the risk of misinterpretation of Pillar 3 information – and breakouts were held on these three topics.

Both reports are short and to the point and will provide valuable guidance to participants preparing for their publication of Pillar 3-required information – the adequate disclosure of information that should be made to allow market participants to assess an entity's capital adequacy: high level information on the scope of application, capital, risk exposures and risk assessment processes.

SEPA

SEPA goes live

The first stage implementation of the single euro payments area (SEPA) - which aims to make cross-border payments as cheap as domestic transactions - has gone live with the official launch of the SEPA payment instrument for credit transfers.

The launch of the SEPA credit transfer (SCT) scheme was marked by a high-level meeting organized by the European Commission (EC), the European Central Bank (ECB) and the European Payments Council (EPC) at the Charlemagne Building in Brussels.

The SCT scheme enables euro credit transfers to be made within a maximum of three days, without any deductions from the principal amount.

In a joint statement, the EC and ECB say SEPA is "a natural progression to the introduction of the euro and another major step in realizing the full potential of the single market for Europe".

EBA Clearing is reporting a successful start to its Step2 SEPA credit transfer service on its pan-European automated clearing house (PE-ACH) platform. More than 100 banks tested the new service with EBA Clearing and SIA-SSB in the second half of 2007.

EBA Clearing said that 90 direct participants sent payments through the service on the launch date. Participant banks began submitting payment files to Step2 SCT on 25th January and at the start of the Step2 system, these payments were routed, delivered and cleared.

UK payments association APACS says that although Britain is not in the euro zone, several banks based in the country are joining the SCT scheme from the launch. APACS says the banks involved at this stage account for about 85% of the UK payments market and this is expected to increase over time.

Meanwhile UK transaction processing outfit VocaLink says it has also processed its first SEPA transaction - from Austrian bank Bawag PSK to Fortis in Belgium. A number of major banks - including ABN Amro, Bank of America, Citi, Dexia Bank, Fortis, Lloyds TSB, RBS and Santander - have signed up for the VocaLink €CSM partnership, which provides banks and clients with SEPA-related services.

Citing research conducted by Capgemini, the EC says SEPA could produce savings of up to €123 billion over the next six years. A further €238 billion could be saved if the SEPA platform can be used as an electronic invoicing platform.

Research released by the ECB last year found that banks will incur the most costs in the period where national and SEPA payment infrastructures co-exist. The ECB has urged financial firms to implement SEPA changes as quickly as possible in order to achieve economies of scale as payments revenues begin to drop due to competitive pressures.

However a study conducted by Finextra last year found that European bankers were pessimistic about their ability to meet SEPA deadlines and that most banks do not expect their corporate customers to be fully SEPA-compliant until after 2010.

Only eight per cent of the 100 banks polled by Finextra were fully SEPA-compliant and over half did not expect to be able to meet the initial deadline for SEPA credit transfers.

Denmark

Payment Business Services signs 117 banks to SEPA direct debit offering

Danish payments body Payment Business Services (PBS) says it has signed deals to provide SEPA-compliant direct debit payment processing services to a group of 117 banks in Denmark.

The aim of the Single Euro Payments Area (SEPA) - which was officially launched by the European Central Bank (ECB) at the end of January - is to dismantle cross-border barriers and drive down costs for non-cash payments in the euro zone to the level of domestic transfers.

Although Denmark is not currently in the euro zone, banks and processors in the country - like those in the UK - that do business in the region will need to be SEPA-compliant.

Anders Dam, CEO of Jyske Bank - one of the banks signed up to PBS's SEPA services - says: "Although Denmark currently is not a euro country, we are fully aware where the future market lays. We want to be ready in time, and we welcome that PBS, with whom we have a long well established business relation, is capable of bringing this service to market."

PBS says it is "investing heavily" in its future payment and information systems in order to be able to compete following the introduction of SEPA.

Flemming Jensen, CEO, PBS, says the deal with the 117 banks "represents PBS' initial SEPA effort".

"We are looking forward to continuing and expanding our cooperation with this large group of banks. PBS is sending a clear message: We want to provide SEPA services to banks and their customers - in Denmark and abroad," adds Jensen.

The SEPA initiative is expected to intensify competition and consolidation in the euro zone so that ultimately just a few payment processors will remain. Research released by Accenture last year predicted that following SEPA, debit and credit card schemes will be dominated by MasterCard and Visa, with only four domestic card schemes offering full SEPA payments services.

On 28 January 2008 an important milestone in the SEPA migration process will be reached, with the official launch of the first SEPA payment instrument for credit transfers. The event is being marked by a high-level meeting organized by the European Commission, the European Central Bank and the European Payments Council at the Charlemagne Building in Brussels.

Remittances

India

Money transfer through mobiles soon

Indians working abroad may be able to send money back home through mobile phones before the end of 2008, with Western Union and Bharti Airtel looking launch the service by December.

"We are working to commercialize the mobile money transfer agreement signed with the Bharti Airtel by December 2008," Western Union managing director (South Asia) Anil Kapur said in New Delhi on Monday.

The company, he said, is working out the modalities for giving effect to the money transfer scheme through mobile phones that will initially be launched for some selected countries.

Western Union and Bharti Airtel had signed an agreement in October last year to develop a scheme on pilot basis for cross-border money transfer through use of mobile phones.

India has emerged as the largest recipient of overseas remittances over the years, Kapur said, adding that "though the number of overseas Chinese is much more, India receives significantly higher remittances than China."

The country receives bulk of remittances from North America, followed by the Gulf region and countries like Malaysia, Singapore and Australia.

Philippines

Western Union pilots mobile remittance system

Money transfer operator Western Union is teaming with two telcos in the Philippines - Globe Telecom and Smart Communications - to develop and pilot mobile international remittance services.

The news services - which are part of a pilot program from Western Union and the international trade group of mobile phone operators GSMA - will enable people overseas to send remittances to recipients in the Philippines.

Western Union cites research prepared by the Commission on Filipinos Overseas that suggests 44% of households in the Philippines have a relative working abroad.

Commenting on the initiative Ferdinand Dela Cruz, head, consumer wireless business group, Globe Telecom, says: "This relationship with Western Union will increase the accessibility and lower the cost of micro-remittances, which will greatly benefit Filipino overseas workers and their families."

Dela Cruz says the agreement will see Globe Telecom's SMS text-based GCASH service - which includes an electronic wallet feature that lets users send and receive cash and make payments - to a global network of send and receive locations through Western Union."

Meanwhile, Smart already has an established mobile financial service platform linking local bank accounts to mobile handsets. The telco says over seven million of its 30 million subscribers use its Smart Money system, with nearly two million of these cardholders.

Commenting on the Western Union alliance, Napoleon Nazareno, Smart president and CEO, says: "This agreement is in line with Smart's thrust to continuously develop convenient mobile remittance channels and communications services for overseas Filipino workers."

Western Union has already partnered Indian telco Bharti Airtel on a similar mobile remittance system as part of its agreement with the GSMA.

United States

Citi releases white label remittance platform

Citi has released QuikRemit, a white-label remittance platform previously supplied by money transfer outfit PayQuik, which was acquired by the US bank in January.

The QuikRemit platform can be used for both online and in-branch remittances and has distribution and foreign exchange capabilities spanning more than 90 countries.

Citi says banks, corporations and money transfer firms can use the platform to offer customers and employees a secure and compliant service for international funds transfer.

The US bank acquired the technology when it bought out remittance outfit PayQuik - which provides services to banks, credit unions and money transfer operators - for an undisclosed sum last month.

Paul Galant, CEO of Citi's global transaction services business, says Citi has offered global remittance services to clients since 2006 and this launch "will accelerate our growth in a strong and dynamic market".

"The remittance market, traditionally dominated by money transfer organizations, is seeing increased participation by banks who can offer a wide distribution network and a safe, secure and private service," says Galant. "Citi's QuikRemit Service enables financial institutions and corporations to offer these benefits to their clients."

The US bank cites Aite Group's March 2007 report which suggests that global remittance volumes will reach $5 trillion by 2010.

Citi is one of a number of financial institutions that has sought to cash in on the remittance opportunity.

In particular, a number of firms - including Visa, Wells Fargo, Bank of America and HSBC - have moved to tap into the Latin American money transfer business and have launched services aimed at the Hispanic community in the US.

Meanwhile money transfer operator Western Union and MasterCard are working on separate projects with GSMA - an international trade group of mobile phone operators - to develop the commercial and technical specifications for global mobile remittance services.

Legal Issues

China

Re-trial for ATM thief given life sentence

A Chinese court will re-hear the case of a man who was handed a life sentence for taking funds from a faulty cash machine which deducted just Yn1 from his account for every Yn1,000 withdrawn from the ATM.

According to local press reports, Xu Ting, 25, withdrew nearly Yn175,000 - around US$24,000 - in 171 transactions from a malfunctioning ATM located in Guangzhou in May 2005.

Xu also allegedly told a friend of the fault who withdrew Yn18,000 from the unit. Xu's friend turned himself in and was jailed, says the report, but he remained "on the run" for a year before being arrested.

Following the trial last year, Guangzhou Intermediate People's Court sentenced Xu to life imprisonment for the crime and ordered him to turn over his personal assets.

Under the criminal law, people who steal more than Yn100,000 from a bank face a life sentence or the death penalty, says the press report.

However recently the higher Guangdong High People's Court reportedly overturned the sentence and other charges due to "ambiguous" and "insufficient evidence".

The lower court is now set to re-hear the case. Lawyers for Xu have submitted a letter to the intermediate court requesting his release on bail pending the trial.

United Kingdom

Maestro loses Internet domain name fight

A British man has won his legal battle to hold onto the maestro.co.uk Web domain name, despite a challenge to his ownership by Maestro International, MasterCard's debit card scheme.

Maestro International lost an earlier case in September 2007 against Mark Adams, and had lodged an appeal with UK domain name registrar Nominet. The appeal was heard in December 2007, but Nominet's ruling has only just been published.

Adams is a Milton Keynes-based Web domain name dealer and Website designer.

Maestro International argued that Adams had registered a series of domains that were close to or the same as recognized brands, and that maestro.co.uk was just another example of this practice, known as "cybersquatting." Adams's domains include beverlyhillscop.co.uk, popidol4.co.uk and forrestgump.co.uk.

UK domain registrar Nominet said it accepted that, while Adam's domains might be considered an attempt to copy established

brands, it was not possible to infer that his ownership of maestro.co.uk was similarly abusive.

Adams told Nominet he planned to use the Maestro.co.uk Website for music downloads and educational services.

Nominet said that Adams was entitled to keep the Maestro domain because he was guilty of nothing more than registering the name ahead of Maestro International. It said that Maestro International was unable to demonstrate that the registration was abusive.

The word 'Maestro' itself is generic, and is widely used in Website domain addresses, Nominet said.

Financial Services Authority considering tougher bank regulation

The United Kingdom's financial operating philosophy always has been one of less regulation. However, fallout from the current sub-prime credit crisis, which has grown to global proportions, could spark a new approach. Specifically, UK regulators are weighing changes that could require banks to deploy reporting technologies that will keep regulators abreast of problems in a timelier manner.

The spur to action in the UK came this past September, when mortgage lender Northern Rock was forced to appeal to the Bank of England for emergency funding. The event caused depositors to panic and withdraw their funds - "an event that is called the first depositor run on a U.K.-based bank in over 100 years," says Bob McDowall, senior analyst, international practice, TowerGroup (Needham, Mass.).

Unlike the FDIC and other regulatory agencies in the US, "The Financial Services Authority [along with the U.K. Treasury and Bank of England] historically used broad guidelines, rather than detailed rules, for the banking industry to follow," says Paul Henninger, director of product management, fraud solutions, for Actimize (New York).

However, now this approach is blamed for "what is called 'a collective failure of responsibility and action' among the U.K. Treasury, the Bank of England and the FSA," which are considered responsible for detecting errors in Northern Rock's business operations, TowerGroup's McDowall explains.

To prevent similar incidents in the future, the U.K. government is proposing that the FSA should have more power to require more-detailed, frequent financial information and disclosures from banks. The government could propose this legislation by the end of the first quarter, and a law could be passed by the spring. Once the proposed law is enacted, however, "It could take up to 12 months to determine whether reporting requirements should be more stringent," McDowall adds.

If the law indeed is passed, banks may be required to upgrade or add new systems to support transaction monitoring and auditing processes. These mandatory upgrades also will force financial institutions to dedicate more of their IT budgets to compliance remediation.

"Increased regulations almost always result in increased IT spending, since most regulations require that financial institutions monitor a range of high-risk or highly critical activities, and the need to report on problems within those activities," Actimize's Henninger explains. "However, it will be the penalties, not the regulations that will really result in major changes in the way banks operate."

The FSA is expected to focus initially on business areas, including market abuse and insider trading, customer data security, and liquidity risk.

Although banks may argue that they already have solutions in place to protect and analyze data, or to present information collected during audits, their existing systems may not suffice going forward. "Whether analytics will be

required for monitoring high-risk transactions and processes depends on how serious the regulators are about identifying problems early," Henninger says.

"The new powers could demand that banks upgrade systems or add solutions that better protect customer data and other sensitive information," he says. "While this is already a concern among the FSA, the organization may simply want banks to deploy sound solutions that ensure data will not end up in the wrong hands."

(such as those contained in Basel II) and into an understanding of operations risk management & mitigation as a value added proposition, increasing the bank's profitability and structural strength.

Who should attend?

- This course is intended for Executive Management, Senior Personnel, Operational Staff and Line Personnel whom are responsible for the operations risk management program in their respective business unit/division/branch or for carrying out the implementation of that program.
- This course also is an ideal introduction for Central Bank staff involved in oversight issues who require a strong Operations Risk foundation.
- Course includes 2 major case studies (including the latest SocGen developments)

Act now!

- Register now for this superb new course!
- Places limited, so don't be disappointed!
- Don't miss out on this fantastic opportunity!

To download a full course description! (Click the link below)

- **Beyond Compliance**

Or request a full brochure by e-mailing us at courses@citadeladvantage.com