Citadel Advantage

CA Digest

PAYMENTS NEWS YOU CAN USE

Biweekly Digest of Payments & Related Information from around the World

No: 149 **Date: 2nd July 2008**

In Focus

Banking regulators move to tackle liquidity risk

The Basel Committee on Banking Supervision has issued new draft guidelines for the management and supervision of liquidity risk, aimed at making the global banking system more resilient and addressing weaknesses revealed by the credit crunch.

The Committee - which is part of the Bank for International Settlements (BIS) - said in April that it would publish for consultation a new set of "global sound practice standards" for liquidity risk management after the credit crisis "revealed significant risk management weaknesses at banking institutions".

The new draft principles represent a substantial revision of the Committee's liquidity guidance published in 2000 and reflect lessons learned from the financial market turmoil.

The primary objective of the new guidance is to raise banks' resilience to liquidity stress. Among the measures put forward are the need for "governance and the articulation of a firm-wide liquidity risk tolerance" and more effective liquidity risk measurements, including the capture of off-balance sheet exposures and "other contingent liquidity risks that were not well managed during the financial market turmoil".

The need for banks to improve liquidity cushions and for regular public disclosures of a bank's liquidity risk profile are also highlighted, along with the need for stress tests that cover a "variety of institution-specific and market-wide scenarios" and are linked to the development of contingency funding plans.

The principles also aim to boost the role and expectations of supervisors, including the need for timely intervention to address deficiencies and the importance of communication with other supervisors and public authorities, both within and across national borders.

Nout Wellink, chairman of the Basel Committee and president of the Netherlands Bank, warns that it expects banks and supervisors to implement the enhanced principles "promptly and thoroughly".
"We will vigorously assess the degree to which the principles are implemented," says Wellink.

The group is inviting comments on its draft guidelines by 29 July.

Risk Management Tips

Citadel Advantage puts you in control when managing Operational Risk

Business Continuity Planning

Does your bank regularly assess its business continuity plans and review the adequacy of these plans for a partial or complete failure of each retail payment system?
Do these plans include:

- Recovery of all required components linking the bank with third-party network switch, gateway, or related third-party data centers and card processors?
- Information relative to the volume and importance of the retail payment system activity to the bank's overall operation?
- Provisions for acceptable store and forward procedures to protect against loss or duplication of data and to ensure full recovery within reasonable time periods?
- Stand-in arrangements with other banks included within the plan, allowing for interim card processing in the event of an outage?
- Adequate testing of plans accounting for various recovery scenarios?

Special Report

Unbanked will drive mobile finance – study

More than 41.5 billion financial transactions will be carried out by mobile phone by the end of 2011 as unbanked consumers adopt the technology to access banking services, according to a study by Juniper Research.

Juniper predicts that 612 million mobile phone users will conduct financial transactions with their handsets by 2011, generating over $587 billion. Annual global mobile banking transactions will soar from 2.7 billion in 2007 to 37 billion by 2011.

The study cites the millions of mobile phone users in developing countries who do not have bank accounts or credit cards as a massive potential market.

The remittance and money transfer market will prove particularly popular, although Juniper warns providers that issues surrounding legislation designed to combat money laundering make it a costly exercise.

The Far East and China will see the biggest adoption, with 250 million mobile phone users conducting financial transactions by 2011.

In the developed world, Juniper predicts teenagers who cannot access regular financial services will drive adoption.

The figures are conservative compared to a report published earlier this year by market research firm IMS Research which predicted that 884 million users of contactless mobile payments, mobile banking and over the air (OTA) transactions will complete a total 62 billion transactions between them in 2012.

UPCOMING CITADEL ADVANTAGE TRAINING COURSES

NEWLY added items are highlighted in BLUE

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

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

OUR COURSES OFFER THE IDEAL SOLUTION TO YOUR OPERATIONS TRAINING NEEDS

Dates	Course	Location	Sponsor	Links
9, 10 & 11 July 2008	OPERATIONS RISK MANAGEMENT – BEYOND COMPLIANCE – A VALUE ADDED APPROACH	Athens	**Citadel Advantage**	***Details***
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***
18, 19 & 20 August 2008	BUSINESS CONTINUITY & SCENARIO PLANNING	Johannesburg	**Citadel Advantage**	***Details***
21 – 22 August 2008	MANAGING RISK IN WHOLESALE & LARGE VALUE PAYMENT SYSTEMS	Johannesburg	**Citadel Advantage**	***Details***
25, 26 & 27 August 2008	MANAGING OPERATIONS RISK – BASEL II & BEYOND	Moscow	**Citadel Advantage**	***Details***
28 & 29 August 2008	REDUCING RISK IN FOREIGN EXCHANGE SETTLEMENT	Moscow	**Citadel Advantage**	***Details***
10 – 11 September 2008	INTERNATIONAL PAYMENTS	Singapore	In conjunction with Marcus Evans	Details coming soon
24 - 26	BUSINESS CONTINUITY & SCENARIO	Hong Kong	In conjunction	***Details***

September 2008	PLANNING FOR BANKS		with Ethan Hathaway	
27, 28 & 29 October 2008	OPERATIONS RISK MANAGEMENT – BEYOND COMPLIANCE – A VALUE ADDED APPROACH	London	In conjunction with Marcus Evans	Details coming soon
18 – 19 November 2008	MANAGING RISK IN WHOLESALE & LARGE VALUE PAYMENT SYSTEMS	London	In conjunction with Marcus Evans	Details coming soon

Operations Risk

Canada

Toronto police bust ATM skimming gang

Police in Toronto have broken up a sophisticated ATM skimming ring that used a network of 'debit card laboratories' to defraud bank customers of hundreds of thousands of dollars.

The swoop on the Toronto crime ring followed a six-week surveillance operation and resulted in the arrest of eight local people. The gang used portable card skimmers to capture customer data at the cash machine for later download and transfer to counterfeit cards.

The police raid on "two sophisticated labs" netted $120,000 cash and led to the arrest of eight suspects. Computers, skimmers, card−readers, molding machines, embossers, tippers, counterfeit cards, cameras, overlays and valances, tools and two−way communications devices were also seized.

Theft and counterfeit payment cards have been a growing problem for the Canadian banking industry, which is making a gradual transition to chip-based technology. Police say over $100 million was lost to this type of activity in 2007, which involved 159,000 card holders.

United Kingdom

Security fears raised over London's Oyster card

New fears have been raised about the security of London's contactless Oyster travel card after Dutch scientists managed to use a cloned card to travel around on the city's underground for free.

According to press reports the researchers from Radboud University used a commercial laptop to reverse the algorithmic code of NXP's Mifare Classic RFID chip, which is used for millions of smart cards around the world.

They then cloned a swipe card and accessed a Dutch public building before moving onto London and carrying out the same process with an Oyster card and travelling on the underground for the day before restoring its balance.

The team is also thought to have managed to carry out a denial of service attack on a tube gate.

Transport for London says it runs daily tests for cloned and fraudulent cards and insists that any

fraudulent cards would be stopped within 24 hours of being discovered.

Researchers from the University revealed in March they had discovered a serious security flaw in Mifare Classic chips relating to an encryption algorithm. They say there is a "relatively easy" method to retrieve cryptographic keys, which does not rely on expensive equipment.

The researchers informed the Dutch government of their findings in March because "national security issues might be at stake".

The Dutch authorities have postponed plans for a transport payment system similar to the Oyster card until the issue is fixed and are replacing all 120,000 swipe cards used by civil servants to enter government building and has posted armed guards outside the offices.

The latest concerns over the security of RFID technology follow a demonstration by security expert Adam Laurie at the Black Hat 2008 conference earlier this year.

At the conference Laurie used his new EMV Chip And PIN credit card reading script, called ChAP.py, to pull the name, account number and expiration date from an audience member's RFID enabled American Express card - without removing the plastic from the victim's wallet.

Woman cons cashier with £20 note from Santa Christmas Bank

A Scottish court has heard how a woman managed to dupe a cashier into accepting a hand-made fake £20 note that stated it was from the 'Santa Christmas Bank'.

The note featured a picture of Santa and his reindeer and promised to pay the bearer nothing. Santa himself was listed as chief operating officer with a North Pole address.

According to local newspaper "The Daily Record", the fake note was so poor that it was not even referred to as a counterfeit in the charge but as a "piece of paper".

Yet on January 16, Stacy Rice, 27, from Dundee, managed to pay a cashier at a gym with the dodgy note and even got change from her purchase. Rice was only caught when bosses at the Fitness First gym in Dundee spotted it was a fake.

Rice admitted fraud at Dundee Sheriff Court and was fined £75. The court heard she became desperate for money after delays in receiving welfare payments. According to reports, Sheriff Alistair Duff said the most astonishing thing about the case was that Rice got away with the scheme.

Rick Brown from Fitness First told reporters that all staff have been given "refresher training" and have gone through security procedures "because we don't want this to happen again".

Merchant Securities fined for slack security

The UK's Financial Services Authority (FSA) has hit stockbroker Merchant Securities with a £77,000 fine for failing to protect customers from the risk of identity fraud.

The FSA - which discovered the "weak data security controls" during a routine visit to the firm in September 2007 - says this is the first time it has fined a stockbroker for slack security.

The watchdog says Merchant Securities did not have proper procedures in place to identify customers over the phone. Instead the company relied on staff recognizing customers' voices and chatting with customers about "personal matters such as holidays or hobbies".

The broker also included personal account numbers in routine letters. This data could be used - with a customer's name - to access account information.

Another lapse saw back-up tapes containing unencrypted customer information stored

overnight in a bag at the home of a member of staff.

What's more, the firm made no effort to address the risk involved in staff being able to use instant messaging and Web-based email.

"It is unacceptable that despite increased awareness of data security issues, a firm should be so careless about its systems for protecting customers' personal details," says Margaret Cole, director of enforcement, FSA. "Reducing financial crime in the UK is a priority for the FSA and our recent data security report showed that many firms still need to do more to get it right. We will not wait until information has been lost or stolen before taking action against a firm. The level of the fine for a firm of this size should serve as a warning to others to take data security seriously."

Despite the slack security, the FSA says there is no evidence that customer data had been lost or stolen.

Merchant Securities was given a 30% discount on the fine - which would have been £110,000 - for co-operating with the FSA's investigation.

In April the FSA warned UK institutions to improve their data security practices after a review of systems and controls at 39 firms uncovered slipshod practices at banks, building societies, insurance companies and financial advisers.

The watchdog said "many firms" still underestimate the risk of data loss and fraud to their businesses and especially to their customers. This includes senior management at firms not recognizing the value of their customers' data to fraudsters or that staff could pose a similar threat to data security as that posed by computer hackers and burglars.

United States

Web personal finance sites – a potential security risk

"Cool" personal finance Websites such as Banzai, Mint, Wesabe and others offer a look into the future of online banking, but also open the door for ID theft, warns TowerGroup.

Non-bank online personal finance sites offer a new take on traditional account aggregation services. By using Web 2.0 community-sharing concepts such as Web forums and blogs, they allow individuals to interact, share, learn, and belong to a like-minded community.

"Consumers are often drawn to these new offerings by attractive interfaces and compelling market campaigns," says TowerGroup analyst George Tubin.

However, most of the new sites pose a security risk and are likely to become the next target for phishers and other fraudsters, Tubin cautions. This is because they use only single-factor authentication - user name and password - to protect customer information.

TowerGroup believes that the US Federal Trade Commission (FTC) should step up regulation of these online sites. Specifically, it should impose the federal banking regulators' 2005 FFIEC (Financial Institutions Examination Council) guidance on online authentication. Notwithstanding the security concerns, Tubin says, consumer banks will want to move into this space and "will either adopt similar capabilities themselves, partner with new independent players, or acquire them."

Banks could offer a compelling service by combining their existing products, services and security capabilities with the fresh approach of the new online personal finance sites, Tubin says.

SEC charges two former Bear Stearns hedge fund managers with fraud

The Securities and Exchange Commission (SEC) has charged two former Bear Stearns Asset Management (BSAM) portfolio managers for fraudulently misleading investors about the financial state of the firm's two largest hedge

funds and their exposure to subprime mortgage-backed securities before the collapse of the funds in June 2007.

The SEC's complaint alleges that when the hedge funds took increasing hits to the value of their portfolios during the first five months of 2007 and faced escalating redemptions and margin calls, then-BSAM senior managing directors Ralph R. Cioffi and Matthew M. Tannin deceived their own investors and certain institutional counterparties about the funds' growing troubles until they collapsed and caused investor losses of approximately $1.8 billion.

The SEC's action was conducted through its Enforcement Division's subprime working group, which is aggressively investigating possible fraud, market manipulation, and breaches of fiduciary duty that may have contributed to the recent turmoil in the credit markets.

In a related criminal action, the U.S. Attorney's Office for the Eastern District of New York announced the indictment of Cioffi and Tannin on conspiracy and fraud charges.

"Hedge fund managers owe serious obligations to investors in their funds, and the Commission will be unyielding in its commitment to vigorous investor protection by enforcing the securities laws against them whenever warranted," said SEC Chairman Christopher Cox. "Hedge funds are by no means unregulated when it comes to fraud. Those who commit fraud at the expense of investors will always be the target of a relentless SEC."

Linda Chatman Thomsen, Director of the SEC's Division of Enforcement, said, "Hedge fund managers remain subject to the same prohibitions against fraud as other market participants. When they choose to make public statements, they must not speak falsely or omit material information."

Antonia Chion, Associate Director of the SEC's Division of Enforcement, added, "Hedge fund managers cannot lie to their own investors as alleged here, simply because those investors happen to be more sophisticated than the general public. Particularly in times of poor performance or market difficulty, even sophisticated investors look to fund managers to speak truthfully to them."

According to the SEC's complaint the Bear Stearns High-Grade Structured Credit Strategies Fund and Bear Stearns High-Grade Structured Credit Strategies Enhanced Leverage Fund collapsed after taking highly leveraged positions in structured securities based largely on subprime mortgage-backed securities. Cioffi acted as senior portfolio manager and Tannin acted as portfolio manager and chief operating officer for the funds, and they misrepresented the funds' deteriorating condition and the level of investor redemption requests in order to bring in new money and keep existing investors and institutional counterparties from withdrawing money. For example, Cioffi misrepresented the funds' April 2007 monthly performance by releasing insufficiently qualified estimates - based only on a subset of the funds' portfolios - that projected essentially flat returns. Final returns released several weeks later revealed actual April losses of 5.09 percent for the High-Grade Structured Credit Strategies Fund and 18.97 percent for the High-Grade Structured Credit Strategies Enhanced Leverage Fund.

The SEC's complaint alleges that Cioffi and Tannin also misrepresented their funds' investment in subprime mortgage-backed securities. Monthly written performance summaries highlighted direct subprime exposure as typically about 6 to 8 percent of each fund's portfolio. However, after the funds had collapsed, the BSAM sales force was ultimately told that total subprime exposure - direct and indirect - was approximately 60 percent.

The SEC further alleges that Cioffi and Tannin continually exaggerated their own investments in the funds while using their personal stake as a selling point to investors. Tannin repeatedly told investors, directly and through the Bear Stearns sales force, that he was adding to his own stake

in the funds in order to take advantage of the buying "opportunity" presented by the funds' losses. Tannin never actually added to his investment. He mocked as "silly" at least one investor who sought to redeem instead of following Tannin's supposed example. Meanwhile, Cioffi redeemed $2 million, which was more than one-third of his personal investment in the funds at the end of March 2007. Cioffi transferred it to another BSAM fund that he described as "short sub prime," which he knew was profitable at the time.

The SEC alleges in its complaint that Cioffi and Tannin violated Section 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5. In its complaint, the SEC seeks permanent injunctive relief, disgorgement of all illegal profits plus prejudgment interest, and the imposition of civil monetary penalties.

Need to improve configuration of the management of key financial systems

The Federal Deposit Insurance Corporation (FDIC) has made significant progress in mitigating previously reported information security weaknesses. Specifically, it has corrected or mitigated 16 of the 21 weaknesses that GAO (Government Accountability Office, which is the audit, evaluation, and investigative arm of the United States Congress) had previously reported as unresolved at the completion of the 2006 audit. For example, FDIC has;

- Improved physical security controls over access to its Virginia Square computer processing facility,
- Instructed personnel to use more secure e-mail methods to protect the integrity of certain accounting data transferred over an internal communication network, and
- Updated the security plan and contingency plan of a key financial system.

In addition, FDIC stated it has initiated and completed some actions to mitigate the remaining five prior weaknesses.

Although FDIC has made significant progress improving its information system controls, old and new weaknesses could limit the corporation's ability to effectively protect the confidentiality, integrity, and availability of its financial systems and information. In addition to the five previously reported weaknesses that remain unresolved, newly identified weaknesses in access controls and configuration management controls introduce risk to two key financial systems. As an example, FDIC did not always implement adequate access controls. Specifically, multiple FDIC users shared the same login ID and password, had unrestricted access to application source code, and used passwords that were not adequately encrypted.

In addition, FDIC did not adequately (1) maintain a full and complete baseline for system requirements; (2) assign unique identifiers to configuration items; (3) authorize, document, and report all configuration changes; and (4) perform configuration audits. Although these weaknesses did not pose significant risk of misstatement of the corporation's financial statements, they did increase preventable risk to the corporation's financial systems and information.

According to GAO a key reason for these weaknesses is that FDIC did not always fully implement key information security program activities. For example, it did not adequately conduct configuration control testing or complete the remedial action plan in a timely manner and did not include necessary and key information. Until FDIC fully performs key information security program activities, its ability to maintain adequate control over its financial systems and information will be limited GAO said.

Citibank linked to ATM breaches

Two men have been charged with making hundreds of fraudulent withdrawals from New

York City automatic teller machines earlier this year, taking more than $750,000 in cash.

In a federal indictment filed in the US Southern District of New York (Citibank Indictment) Yuriy Ryabinin, a 32-year-old Ukranian immigrant and Ivan Biltse, 30, are charged with access device fraud, using stolen information from a computer intrusion into a Citibank server that processes ATM withdrawals. The indictment says Ryabinin and Biltse allegedly "received over-the-internet information related to Citibank customers, which information had previously been stolen from Citibank." They are not being charged with the computer intrusions.

In a related affidavit filed in the same case, the Ukranian immigrant is also accused of taking part in an attack against four iWire prepaid MasterCard accounts in a two-day period last fall. The iWire accounts, issued from First Bank, St. Louis MO, recorded more than 9,000 withdrawals (both actual and attempted) from ATM machines located "around the world" from September 30 to October 1. According to the affidavit, First Bank officials contacted the United States Secret Service on October 3 about the withdrawals. The affidavit (Citibank Complaint), from FBI cyber-crime investigator Albert Murray states the total taken in the caper was $5 million. Ryabinin is charged with taking more than $100,000 of the iWire cash from Brooklyn, NY cash machines. The iWire company contracts with employers that need to pay employees without bank accounts via prepaid cards.

Citibank denies the indictment and affidavit's charge that their server had been breached. "The facts alleged in the indictment about Citibank's systems are not correct. Citibank's servers were not compromised," says Rob Julavits, a Citibank spokesperson. Julavits explains that, earlier this year, Citibank received notice from a third-party transaction processor for the ATM industry that the processor's systems were potentially compromised in late 2007. "As a preventative measure, we notified and reissued new debit cards to those customers whom we believed may have been exposed to increased risk," Julavits says.

The two men were arrested on February 29 and March 5 and await trial. An arrest warrant was also issued on March 5 for Ryabinin's, wife who is also charged in the indictment.

Did You Know?

Correspondent bank	An institution, acting on behalf of other institutions that can settle the checks they collect for other institutions (respondents) by using accounts on their books or by sending a wire transfer. Generally, a provider of banking and payment services to other financial institutions.
Credit card	A card indicating the holder has been granted a line of credit. It enables the holder to make purchases or withdraw cash up to a prearranged ceiling. The credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged based on the terms of the credit card agreement and the holder is sometimes charged an annual fee.

Did You Know?

Credit entry — An entry to the record of an account to represent the transfer or placement of funds into the account.

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

Payment, Settlement & Banking Systems

Dubai

Dubai International Financial Centre to implement real time payments

The Dubai International Financial Centre (DIFC) has signed a Memorandum of Understanding (MoU) with the UAE Central Bank under which the bank becomes the lead regulator for Real-time Automated Payments in DIFC (Rapid).

Rapid is a DIFC initiative to provide a real-time gross settlement (RTGS) payment systems infrastructure within the DIFC to financial institutions operating within the centre and throughout the region.

Sultan Bin Nasser Al Suwaidi, Governor of the Central Bank, said: "As a pioneering system, Rapid looks set to revolutionize payment methods at the region's leading financial centre.

"We are committed to ensuring the reliability and integrity of all financial products and services in the region."

As part of the agreement, the central bank becomes the lead regulator for the payment systems implemented under Rapid and has ultimate responsibility to ensure that Rapid complies with the Core Principles for Systemically Important Payment Systems (CPSIPS) as issued by the Bank for International Settlements (BIS).

Dr Omar Bin Sulaiman, DIFC Governor, said: "We are delighted that the central bank will govern the payment systems implemented under Rapid."

As the lead regulator of Rapid, the central bank will undertake an initial and periodic assessment of Rapid against the CPSIPS criteria and other international best practices.

DIFC will establish and maintain Rapid legally and commercially. It will establish and maintain appropriate governance powers and structures in

compliance with CPSIPS and other best practices.

International

SWIFT to offer corporate access via USB stick

SWIFT plans to launch a new 'lite' interface device at this year's Sibos in Vienna in September, in an effort to ease access to the payments messaging network for low volume financial institutions and SMEs.

The 'Alliance Lite' interface uses a standard Internet connection with a SWIFT -issued hardware security token, which can be provided on a USB memory stick. Once activated, the corporates can send payment instructions via Swift to their financial institutions in whatever format they want.

A beta version of the product is currently being piloted by over 20 SWIFT customers around the world.

Marc Braet, SWIFT's regional director for Northern and Central Europe, says that SWIFT will be performing demonstrations of Alliance Lite at Sibos. The service is aimed at smaller corporates that don't want to make the investment in connecting to SWIFTNet themselves.

SWIFT also says it intends to develop a similar offering for small to mid-sized fund managers. The new interface device was first trailed by SWIFT CEO Lazaro Campos at Sibos in Boston last year.

Credit crunch to spur IT outsourcing – study

Hit by the credit crunch, banks are looking to outsource operations as a way of deferring investment in their technology infrastructures, according to research from business advisory firm EquaTerra.

EquaTerra says tough economic conditions will contribute to annual spending rises of between seven and eight per cent in financial services outsourcing over the next five to seven years. But the crunch won't be the sole driver of spending. Although in the short term banks will increase spending on outsourcing in response to current market challenges, in the longer term spending will be driven by the need for business process improvement and market innovation, especially as firms look to take advantage of globalization.

"Financial services firms understand they need to reduce complexity across the board to lower costs," says Stan Lepeak, EquaTerra's managing director of research. "A growing need to customize new product and service offerings to capitalize on emerging markets is adding urgency for operational innovation."

EquaTerra says the majority - 64% of financial services executives polled for its survey, which was conducted by the Economist Intelligence Unit, believe rising income levels in developing regions of the world are creating a lucrative pool of new investors, spurring new-market expansion. But this window of opportunity coincides with continued volatility in the global economy. EquaTerra says financial services firms will explore new outsourcing strategies to tackle both these challenges.

"Management and delivery of middle and back office business processes is a prime target for innovation" says John Boyle, financial services sector lead at EquaTerra. "Financial services firms could significantly benefit from alternative service delivery models like offshore captives or outsourcing to more efficiently and effectively deliver these services."

The EquaTerra research backs up a UK study released earlier this week which predicted the credit crunch will drive a wave of outsourcing and offshoring in financial services as cash becomes tighter and banks look to cut costs.

A survey of 70 British Bankers' Association (BBA) members released by Management

Consultancies Association (MCA) found 41% of respondents expect to increase outsourcing levels.

Netherlands

Dutch supermarket pilots fingerprint payments

Dutch supermarket chain Albert Heijn is teaming with European payments processor Equens to test fingerprint scanning technology as an alternative to card and cash payments at the check-out.

Shoppers participating in the new service - called Tip2Pay - will be able pay for purchases by placing their fingertips on a reader at the point-of-sale. The payments will then be processed by Equens.

Customers who want to use the technology will need to provide proof of identification and a debit card before having their fingerprints scanned, says Equens. Customers' names, addresses, bank account numbers and loyalty card details will then be registered in accordance with Netherlands privacy laws.

Albert Heijn and Equens are conducting the six month biometric payments pilot in consultation with biometric specialists IT-Werke, which has implemented the technology at German supermarket chain Edeka.

Equens says the trial - thought to be the first in the Netherlands - is being conducted to test customer reaction ahead of a wider roll out of the technology.

"We regularly test new payment concepts among our customers. We only continue their development if they are received with enthusiasm," says Jan de Heij, innovation manager, Albert Heijn.

South Africa

Insurer introduces SMS fraud tip-off system

South African insurer Santam is implementing mobile phone messaging technology from US-based Clickatell to launch a text-based fraud reporting system.

The text system enables people that are involved in, aware of or witnessing an insurance scam to anonymously tip the insurer off by sending an SMS text message. Clickatell says the use of its text message infrastructure helps Santam to respond quickly and appropriately to reported incidents, reducing the probability of fraudulent or false claims being paid out.

Jerry Chetty, head of forensic services, Santam, says: "We expect our text-based fraud tip line to become the de facto standard across the insurance industry. We expect it will be an efficient and reliable form of communications as the immediate nature of SMS is providing us with the ability to quickly act on fraud tips and maintain high levels of service. We anticipate that it will evolve from receiving text only messages to also be able to receive photos and video clips of unethical behavior as they occur."

"SMS has proven itself to be an efficient and reliable form of communications in the financial services sector and has received widespread adoption due to its immediate, real-time relevance characteristics," adds Pieter de Villiers, CEO of Clickatell.

In addition to the fraud tip-off service, Santam has been working with Clickatell to bolster its corporate call centre to reach customers via SMS more effectively at a lower cost, says the vendor.

United States

MasterCard goes mobile with new partnership

MasterCard is partnering with m-payments technology firm Obopay to create MasterCard

MoneySend, a mobile person to person (P2P) payment service.

The service will be offered to US banks which issue MasterCard-branded cards. It will be usable with credit, debit or prepaid products, according to MasterCard.

MasterCard says it is targeting the increasing number of US consumers who are using their cell phones for banking and mobile payment transactions. According to TowerGroup, a research firm owned by MasterCard, the number of US m-banking users has grown fivefold to 5.7 million today from 1.1 million a year ago.

MoneySend users will be able to send and receive funds through any cell phone that they register with the service. A security feature of the service is that it uses cell phone numbers rather than card account numbers to make and receive payments.

MasterCard and Redwood City, California-based Obopay say they will launch MoneySend with MasterCard's financial institution customers in the near future. "We will begin testing the new service in the fourth quarter of 2008, and anticipate a commercial rollout early in 2009," a MasterCard spokesperson said. "We've just announced the partnership to develop MoneySend, so we don't have any users as yet. We will announce them (users) publically as we sign the contracts."

Basel II

United States

Fed Board proposes rule for calculating risk-based capital requirements

The Federal Reserve Board has proposed a rule for public comment that would implement certain of the less-complex approaches for calculating risk-based capital requirements that are included in the international Basel II capital accord.

The proposal, known as the standardized framework, would be available for banks, bank holding companies, and savings associations not subject to the advanced approaches of Basel II. Under the advanced approaches rule, which took effect April 1 and is mandatory only for large, internationally active banking organizations, banking organizations are required to develop rigorous risk-measurement and risk-management techniques as part of a new risk-sensitive capital framework. The standardized framework also seeks to more closely align regulatory capital requirements with institutions' risk and should further encourage improvements in their risk-management practices.

"The increased risk sensitivity of the standardized framework is aimed at both enhancing safety and soundness for the wide range of institutions that will not be adopting the advanced approaches of Basel II and fostering competitive equity for these institutions," said Federal Reserve Board Governor Randall S.

Kroszner. "Recognizing the diversity of banking organizations in the United States, we want to provide these banks the option of using a more updated capital framework without unduly increasing regulatory burden."

The proposed standardized framework addresses a number of areas including:

- Expanding the number of risk-weight categories to which credit exposures may be assigned.
- Using loan-to-value ratios to risk weight most residential mortgages to enhance the risk sensitivity of the capital requirement.
- Providing a capital charge for operational risk using the Basic Indicator Approach under the international Basel II capital accord.
- Emphasizing the importance of a bank's assessment of its overall risk profile and capital adequacy.
- Providing for comprehensive disclosure requirements to complement the minimum capital requirements and supervisory process through market discipline.

The Federal Deposit Insurance Corporation has voted to issue the interagency notice of proposed rulemaking (NPR) on the Basel II standardized framework for public comment. The Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS) also are considering the NPR. The Board authorized the staff to publish the NPR in the Federal Register for public comment after the other agencies complete their approval processes. For the OCC and OTS, that includes review by the Office of Management and Budget. Comments will be accepted for 90 days from the date of publication in the Federal Register.

Remittances

Fiji

Remittances 'a money laundering target'

The remittance sector is being targeted in Fiji for conducting money laundering transactions, the Fiji Financial Intelligence Unit (FIU) has said. The FIU (whose mission is to assist in the detection, investigation and prosecution of money laundering and terrorist financing offences) said this was an emerging trend in suspicious transactions reports (STRs).

The transactions included channeling of proceeds of criminal activities into the country and remittance of funds out of Fiji to circumvent exchange control restrictions.

The FIU said that another emerging trend found in the reported STR cases was the falsifying of trade documents such as purchase invoices and customs entry form.

In addition, the FIU said that Fiji has also recently been used as a target by fraudulent and bogus investors because there has been increase in the number of fraudulent investment proposals with the involvement of locals and foreigners. There has also been forgery of payment instruments such as bank cheques. The

STRs continuing trends include the transfer of funds from one bank account to another.

The transfer of funds from one common source continues to increase, which appears to be a method of violating requirements under the immigration laws.

The Americas

Remittances to region slow

Stricter immigration laws and an economic downturn in the United States caused a slowdown of remittances sent to Latin America and the Caribbean last year.

In 2007, Latin American and Caribbean immigrants sent a total of US$66.5 billion back to their home countries, according to the Inter-American Development Bank (IADB).

Even though it was 6.7 percent more than in 2006, when remittances totaled $62.3 billion, Donald F. Terry, manager of the bank's Multilateral Investment Fund said since the institute began analyzing remittances in 2000, every year they increased by double-digit percentage points. Remittances in 2006 were 14 percent greater than in 2005.

Most of the money sent home is used for food, clothing, housing and medicine, the IADB says, and they are an important source of income for many countries. In Guyana, remittances comprise 43 percent of the gross domestic product, followed by 35 percent of Haiti's, a quarter of Honduras' gross domestic product and 18 percent of each El Salvador and Jamaica's gross domestic products.

Legal Issues

European Union

MasterCard Europe suspends cross-border interchange fees

MasterCard is suspending the interchange fees it charges for cross-border credit and debit transactions in Europe in order to comply with an EC ruling and avoid heavy daily penalties.

The European Commission (EC) said last December that the multilateral interchange fees (MIF) charged for cross-border transactions made with MasterCard and Maestro debit and credit cards violated EC Treaty regulations.

MasterCard was given until 21 June 2008 to withdraw the fees or incur daily penalty payments of 3.5% of its daily global turnover in the preceding business year.

"We said in December that although we strongly disagree with the European Commission's decision, we would comply with it," says Javier Perez, president, MasterCard Europe.

MasterCard says the transactions affected by its move "amount to less than five percent of MasterCard Europe volume" and it does not anticipate any significant near-term financial impact.

Although MasterCard is complying with the deadline, it says it is continuing negotiations with the EC about "an interchange fee methodology that the Commission services believe is consistent with the decision".

"Despite our having made several proposals to reduce substantially cross-border consumer interchange fees, we have not yet reached an understanding with the Commission services on future steps," says Perez. "Therefore, in order to ensure our compliance with the decision, we have taken this action while we continue discussions with them."

Perez says MasterCard will also continue to "vigorously pursue" its appeal of the decision to the European Court of First Instance, which it filed on 1 March.

In a statement responding to MasterCard's action, EC Competition Commissioner, Neelie Kroes, says: "Irrespective of MasterCard's move to temporarily repeal its cross-border MIF, the Commission will continue to be open to assess any new proposals from MasterCard concerning systems to ensure both efficient payments and a fair share of the benefits for consumers and retailers."

United Kingdom

Bank sues over rumors

Anglo Irish Bank is suing a London-based stockbroker for spreading rumors about Merrill Lynch.

According to the Irish bank's complaint, filed in London's High Court, Mirabaud Securities suggested (falsely) that the US firm had withdrawn a $2 billion credit line. The suit was filed following a call by the UK financial regulator for people to submit cases of traders deliberately manipulating share prices to be submitted to them.

Price fluctuations for the shares of the nation's biggest lender, HBOS, had led the Financial Services Authority to make the call - as these

price movements were apparently caused by rumors and speculation.

Contained in the complaint was a transcript of an email sent by a Mirabaud worker on February 29th, which stated: "Anglo-Irish, ML pull a $2 billion credit line? Rumor."

Anglo Irish terms this message "false and defamatory".

Mirabaud, owned by a private Swiss banking firm, has thus far refused to comment on the case.

Special Report

Rogue trading at Morgan Stanley?

Second quarter results for Morgan Stanley, one of the giants of Wall Street, reveal that the bank has been obliged to write off $120 million due to the potential rogue trading of one of their London office in the interest rate, credit and currency trading team within Morgan Stanley's Institutional Securities business.

In the press release associated with the results, were the words "Within IRCC (Interest Rates, Credit & Currency), continued dislocation in the credit markets resulted in a loss in credit products, compared with a significant gain a year ago. This loss included a $120 million negative adjustment to marks previously taken in a trader's book that did not comply with Firm policies." Overall this unit took a hammering with pre-tax income down to $679M compared with $2,950M in the same quarter last year and a pre-tax margin of 19% compared with last year's 40%.

The press release gives no further information on the incident but London's Financial Times has identified the individual as Matt Piper in the London office and says that he has been suspended on suspicion of increasing the value of his derivatives book to present his performance in a better light. Morgan Stanley told the FT that the mispricing may date back to 2007, was discovered in May and that the FSA have been informed pending an internal review.

This event pales into insignificance compared to the $7 billion impact on SocGen at the beginning of this year (see "How much did the risk management calamity really cost SocGen shareholders?") but it highlights the difficulties that risk management departments have in controlling a large number of traders dealing in esoteric and hard