

# Vanilla PLUS

FEBRUARY/MARCH 2012  
VOLUME 14 ISSUE 1

ISSN 1745-1736

MOBILE  
WORLD CONGRESS  
20-PAGE CEO GUIDE INSIDE

DRIVING PROFITS FOR COMMUNICATION SERVICE PROVIDERS

## TALKING HEADS

**Subex sees CSPs turning to managed services for business optimisation ►**

### CUSTOMER EXPERIENCE

CSPs aim to reset customer expectations for a 4G World

### BILLING & CHARGING

How to create the perfect blend

### INTEGRATING INTELLIGENCE

Redefine customer, content & network intelligence

### 3 SPECIAL SUPPLEMENTS INSIDE!

- Policy, Charging & Personalisation
- Billing & Customer Care
- MWC Barcelona: Devil is in the Data ▼

### MOBILE PAYMENT IN THE NEWS

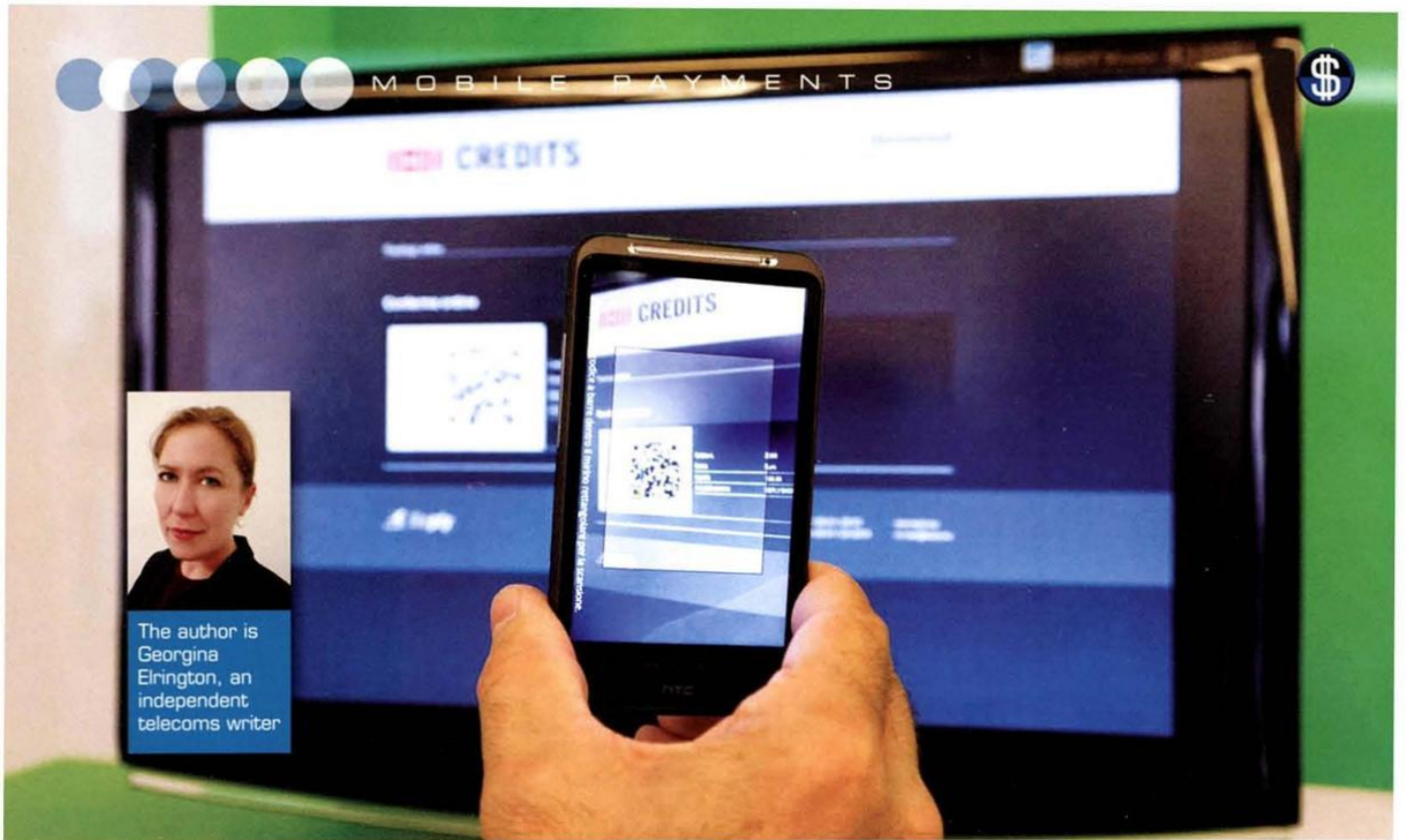
... But it's still not quite time to throw away your wallet ►



**PLUS!**

Contracts, Products, People & Market News • InfoVista, Tekelec acquisitions top US\$800m  
Agents still core of customer care • Research • Sao Paulo to Singapore: BSS & OSS Events  
Europe: Get ready for American message • Latest BSS & OSS News: [www.vanillaplus.com](http://www.vanillaplus.com)





The author is Georgina Elrington, an independent telecoms writer

## M-Payments 'go large' (... but it's not yet time to throw away your wallet)

There's a future of branded applications to extend reach, awareness and customer loyalty as retailers, banks and service providers recognise the mobile money trend. Report by Georgina Elrington



Mark Richards, Actis: E-payments are cheaper and more convenient

The mobile payment market is being accelerated by the greater penetration of smartphones, particularly Android. Technology is streamlining transactions into a one-tap buying experience.

"There is an appetite for these services if they are introduced for everyone," says Nir Shimony, marketing VP at Digimo. However, he goes on to say: "Although everyone is talking about NFC, it requires nearly all consumers to upgrade their handsets before they can use it. Instead of waiting for NFC to happen there are solutions that can work immediately and on any handset for any consumer."

The leading Italian bank, **Banca Sella**, has already adopted **HI Credit's** QR code technology for simple and smart transactions. The HI Credits platform adapts to location-specific purchases; for example, a QR code at a bus stop could substitute a valid travel ticket.

Luigi Cicchese, partner at **Concept Reply** says: "By transforming the modern mobile device into a POS (point of sale), users will be able to perform mobile payments in, for example, high street markets and taxis, where traditionally it has not been possible. Further opportunities will enable users to perform impulsive purchases

through QR scans on flyers, adverts from TV commercials and web banners.

"Retailers hope to improve the interaction with customers, providing them with a new mobile purchase channel characterised by freedom, simplicity and safety of use, as well as increase the number of non-cash transactions and streamline in-store checkout processes," Cicchese adds.

### Opportunity

Mark Richards, partner and head of financial services at **Actis** proffers: "Creating an efficient payments infrastructure requires three things: points-of-sale, cards, and a rational reason for people to use them. Electronic payments are cheaper and more convenient than other forms, and it is therefore unsurprising that the first two of these things are now spreading across Africa."

Richards continues: "In the same way, as points of sale and enabled cards (or mobile devices that can act like cards) are rolled out in developed markets, we believe that users there will see the same fundamental advantages that have already convinced many African consumers."

One example of this is **McDonald's**. Six months ▶



Ray Connolly, eGain: Letting customers communicate on the channels they are most comfortable with (establishes) trust and rapport.

Sponsored by:

[www.redknee.com](http://www.redknee.com)

**REDKNEE**





after enabling NFC payment terminals in all of its 1,200 UK restaurants, the company processed its millionth contactless transaction. Payment time was reduced from seven seconds to just one with authorisation in 0.6 seconds.

Simon Collins, technical director at **Praesidium Services**, a consulting division of **WeDo Technologies** says: "For operators the key to mobile money for 2012 will be to ensure that they are involved in the space. If operators do not create their own products soon, other players in the market, such as banks and credit card companies, will take over and leave operators behind. The areas that pose the greatest risk for operators are the design, security and risk mitigation of mobile money services.

"The key aspect is to thoroughly research both mobile money technology and the potential business risks related to social engineering and manipulation. These are things fraudsters are very good at. The full risk model cannot be evaluated without a thorough understanding of these areas." Says Collins, "So far, we have yet to see the perfect solution; but risk mitigation and control are crucial to the success of mobile money."

### Security

Protection is paramount regarding the safety of personal information that will, inevitably, be stored on mobile phones. A flood of passwords, PINs and other sensitive data will be hitting the airwaves – all at risk from malware, rogue apps and phishing scams.

A survey by **ValidSoft** and **FSTech** into the current sentiment regarding security in the retail banking industry revealed that 71% of respondents thought that UK consumers weren't ready for the mobile wallet; and 47% believed that security was the most likely factor to prevent the adoption of the mobile wallet next year.

Attitudes to mobile banking took a different stance, however; **Datamonitor** expects UK usage to not only match global uptake but also to overtake the internet as the main way for consumers to bank: 63% of banks surveyed believed that m-banking could actually reduce fraud.

Pat Carroll, CEO of ValidSoft, said: "Mobile money transfers will make life more convenient. The example set by successful schemes such as mPesa in Kenya shows what's possible, but with every new technology comes a new risk. Mobiles have been the subject of malware and man-in-

the-mobile threats in the past year. Banks therefore need to up their game on the security front by ensuring that fraudsters can't use any bank details they obtain. This can be done by using a multi-layer authentication process. Voice biometrics can play an important part in the security of mobile money transfer as it strikes the right balance of being sufficiently secure and easy to use."

Another way to authenticate mobile transactions may be fingerprint scanning. **SmartMetric** is looking into such technology which could help raise consumer confidence and, in turn, drive the adoption of m-transactions.

**eGain's** sales director, Ray Connolly, said: "In our experience, service providers considering mobile money products will need to look at the level of customer service they are capable of delivering. Consumers' criteria for selecting a mobile money provider is based on high levels of service and brand reputation, coupled with a strong sense of security and confidence. Customers need assurance that if they have a problem they can solve it quickly: trust is incredibly important to establish and can be your differentiator.

"Letting customers communicate on the channels that they are most comfortable with (email, text, web chat) is an excellent way to establish trust and rapport. Service providers then need to harvest all the information from those multi-channel conversations and use it to deliver a swift resolution to the query or problem." Connolly concludes, "That's really the lesson for the wider world: a focus on customer service strategies is critical if service providers are going to successfully deliver mobile money and transfer services."

The last word goes to Dale Youngs, director - Product Management at **Subex**. He says: "Mobile money and other transaction-based services are growing strongly. We are seeing the emergence of fraud associated with these services, and especially hacking of internet banking applications and associated mobile phone accounts (such as account take-over and SIM-swapping) to perpetrate fraud.

"Even if an exploited weakness is not the operator's fault or their financial liability, the potential reputational damage to the operator can still be enormous. Operators must, therefore, take a strong stance and ensure that these services are absolutely secure, even when they are acting as little more than a 'dumb pipe'." \$



Luigi Cicchese,  
Concept Reply:  
Freedom,  
simplicity and  
safety of use



Pat Carroll,  
ValidSoft:  
mPesa in Kenya  
shows what's  
possible



Dale Youngs,  
Subex:  
Operators must  
ensure that  
services are  
absolutely  
secure



Simon Collins,  
WeDo  
Technologies:  
Challenge to  
operators from  
banks and  
credit card  
providers

### Encourage the market:

- Enable all phones for all users
- Lower the premium SMS rate for m-payments
- Realise customer demand for trust and rapport

Sponsored by:

**REDKNEE**

[www.redknee.com](http://www.redknee.com)

BILLING & CC SUPPLEMENT B15  
VANILLAPLUS FEB/MARCH 2012