Selling biometrics to the retail sector

The retail sector is a potentially 'hot' application area for the biometrics industry. Fraudulent transactions and identity theft are rising at unprecedented levels causing unacceptable losses to retailers. Biometric technology is proving successful in fighting these sorts of crimes, and is attracting attention from some of the world's major retailers. This attention has not yet matured into contracts, however, so for now the use of the technology is confined to small chains of stores, which are using the technology primarily for secure cheque cashing.

Although it is not often an application area to hit the headlines, the retail sector has slowly been emerging as a promising market for vendors in the biometrics industry. As with most niche markets, the vendors that have been most successful, have tuned their systems and product marketing to match the unique needs of the retailers in question.

A small number of vendors have been able to persuade stores to install their systems, not only helping to prove the business case from a fraud perspective, but also, in some cases, helping to increase the stores' revenue thanks to the popularity of the biometric systems with customers.

Retail industry fraud

One of the main reasons that a retailer might consider the use of advanced biometric technology in its stores is to counter the increasing levels of fraud within society. Although estimates of retail losses vary widely, in the USA the **Federal Reserve** believes that cheque fraud and counterfeiting costs business about US$10 billion per year, with the most common type of cheque fraud involving low-value counterfeit cheques drawn against well-known local firms and employers.

Meanwhile the wider problem of identity theft is even more worrying, exploding at a growth rate of about 300% a year, according to **Aberdeen Group**, a Boston-based industry analyst firm. This equates to a financial loss from identity theft of US$73.8 billion in the USA by the end of this year and US$221.2 billion worldwide. The thief will tend to use stolen identity information to obtain credit, merchandise and services in the guise of the person whose information he has stolen. It is a profitable crime too, paying an average of US$9,800 per incident.

Recent experiences at retailers show that the introduction of systems that tie a biometric, such as the fingerprint, to a cheque or transaction, will deter habitual fraudsters from even entering a location. (Note that this does not necessarily stop fraudulent transactions *per se*, as it may just pass on the problem to a neighbouring store. But it does help to eliminate fraud in any single store it is used in and at present that is enough of an incentive for individual stores or chains to investigate the technology.)

Market definition

As noted above, reducing identity fraud is one of the major reasons why a retailer might consider installing a biometric system. Other reasons include the monitoring of employees and increasing customer convenience, by reducing queue times or removing the need for a customer to carry ID, such as a drivers' licence.

Typically biometric technology can either be used in the store itself or to facilitate home shopping and internet purchases. A fuller breakdown includes:

- cheque cashing;
- point-of-sale transactions;
- employee time/attendance;
- loyalty applications;
- access to cash registers and their managerial features;
- online shopping; and
- telephone shopping.

In terms of technology, the dominant biometric is the fingerprint, accounting for almost all the examples *Btt* could uncover (see Table 1). This is no doubt thanks to the technology's low cost, relatively high accuracy and its ease of use. However, keystroke dynamics, facial recognition and dynamic signature verification could also find some success in this market.

Cheque cashing

In the USA (where most of the applications of biometrics in the retail sector have occurred to date), cash is still the most common form of payment, representing almost 40% of transactions. However, the next largest segment, at around one-third of all transactions, was the cheque.

Safeguarding the cheque cashing process has been the biggest market for biometric suppliers to date, with almost all examples in the retail sector applying the technology for this use. The reason is easy to understand. Without scrupulous safeguards, fraudulent cheque cashing can be an easy crime for criminals to perform. On average just over 250 million cheques are returned each year in the USA and some estimate that losses from cheque fraud are growing at a rate of 2.5% annually.

Cheque cashing within retail outlets is major business for some stores, as they make a charge for each cheque cashed. However, the store is often liable for any returned cheques, so undetected fraud can, therefore, cut into the retailer's revenue stream.

For some stores, the result of implementing biometric technology has been impressive, not only cutting down fraudulent transactions, but also increasing the overall number of cheque transactions. For example at **Cardenas Supermarkets** in Ontario, California, a large number of cheques are processed each week – around 10,000 totalling an average of US$5 million. Since the company installed a system from **BioPay**, one of the leading vendors in this market, cheque cashing has increased around 25%.

According to the retailer's general manager, customers are extremely comfortable using the fingerprint-based

Paycheck Secure system, which is relatively non-invasive. Some of the chain's customers are undocumented aliens and a factor that appeals to these customers is the fact that their personal information is used solely for ID purposes, with no sharing of information with the authorities.

To use the system for the first time, a fingerprint template and other information is taken from customers wanting to cash a cheque. This template is stored in a central BioPay database and is subsequently used to verify the identity of the individual. If a cheque is later returned as 'bad', then this is flagged in the system. Central storage of information allows other retailers using the BioPay system to identify fraudulent customers, even if a bad cheque was presented in another store.

Other biometric system suppliers are active in this space such as **Biometric Access Corporation**, although this supplier does not share information between stores.

Point-of-sale

Using biometric technology for authenticating individuals wanting to cash cheques is perhaps just the first step. It is possible that the technology has the potential to reshape electronic payments by linking with existing credit, debit and loyalty card programmes, as well as emerging smart card technology.

One company that is interested in promoting such an approach is **Hypercom**. Hypercom is one of the leading manufacturers of point-of-sale devices for retail environments and has incorporated silicon fingerprint sensor technology from **STMicroelectronics** into its more advanced POS systems.

Under Hypercom's envisaged system, customers enrol at the point-of-sale, having their credentials (such as a driver's licence) verified online in order to validate their identity at the time of enrolment. The enrolled fingerprint template is encrypted and stored centrally, but is linked to a card. For subsequent transactions, the new template along with the unique card identifier is transmitted encrypted and time stamped to the Hypercom database for one-to-one verification. The results are then transmitted back to the terminal. According to Hypercom, the transaction overhead would equate to 300 bytes and 1.5–3 seconds.

This centralised approach has a number of benefits for retailers. According to a spokesperson at **International Biometric Group** (IBG), a US-based consultancy and market research group which held a teleconference on the retail sector earlier this year: "Perhaps the greatest benefit of the centralised approach is that it populates an independent database that can be shared among retailers. The day forward problem – the fact that the biometric system must be populated from the day of deployment forward – is an impediment to the use of biometrics at larger chains. The return on investment may only begin to emerge once a retailer has access to a significant database of enrolees. The availability of a pre-populated enrolment database greatly improves potential return on investment and simplifies life for the customer, who does not need to enrol in various systems."

As well as some of the benefits to this type of approach there are also drawbacks, including:

- databases of biometric data are not likely to be well received by the privacy community;
- a widespread system would almost certainly be voluntary, diluting its potential effectiveness for catching fraudsters;
- companies such as Hypercom are not seen as data storage specialists or as trusted third parties for storing sensitive data.

Alternative arrangements could include cardless biometric transactions with the biometric system either performing a one-to-many search or relying on the consumer remembering a PIN to locate their template on the system. The advantage to this is clearly that the customer would not have to carry a card to perform a transaction, as they would have submitted their various payment mechanism details at initial enrolment (this approach is favoured by **Indivos**, now merged with **Solidus Networks**). This type of system set-up works much better in a closed system environment than in an open system, where the task would be a lot tougher.

From a retailer's perspective, cost could be the single biggest barrier to implementing biometrics. Although they are eager to reduce credit card fraud, they see the cost of installing new equipment at every POS terminal, purchasing the software and managing the integration issues, as well as educating shoppers as significant hurdles.

To some extent, terminal manufacturers are helping to ease this burden by future-proofing their products. **Verifone**, for example, has recently released its *Omni 7000MPD*, a modular payment device that allows retailers to add features and functionality, such as biometrics, as needed.

Despite the detractors to using biometrics at the POS, IBG is positive about the prospects of the market, forecasting a rise in revenue for the ATM and point-of-sale sector from US$9.5 million in 2002 (less than 2% of total biometric industry revenues) to US$285 million by 2007.

Customer	Location	Supplier	Technology	Function
Cardenas Supermarkets	California	BioPay	Fingerprint	Cheque cashing
Fast & Easy	California	BioPay	Fingerprint	Cheque cashing at 30 stores
Food 4 Less	18 stores in USA	BAC	Fingerprint	Cheque cashing
HEB	San Antonio	BAC	Fingerprint	Time and attendance
Home Shopping Network	USA	Nuance	Voice	Caller identification
Hyvee	Five Midwest USA stores	BAC	Fingerprint	Cheque cashing
Kroger	Indiana	BioPay	Fingerprint	Cheque cashing
Kroger	Texas	BAC	Fingerprint	Cheque cashing
Lopez	Texas	BioPay	Fingerprint	Cheque cashing
Malone's Cost-Plus	Texas	BioPay	Fingerprint	Cheque cashing
McDonald's	California	Indivos	Fingerprint	Payment
Men's Warehouse	Houston	Key Source Int.	Fingerprint	T/A, cash register
PAL Market	California	BioPay	Fingerprint	Cheque cashing
Santoni's Surpermarket	Baltimore	BioPay	Fingerprint	Cheque cashing
Thriftway	West Seattle	Indivos	Fingerprint	Payment
United Retail's Jet Stores	South Africa	Biocom	Facial	Payment

Table 1. A selection of retail installations using biometric technology.

Online shopping

It is believed by some that the initial thrust in the biometric retail market will come from payments on the internet rather than at the point of sale. This is because in the internet environment, biometric applications can be facilitated at the card issuer level as opposed to the merchant level, making the payment option available to all online merchants.

The physical retail environment requires merchants not only to become educated and accept biometrics, but to ensure that their point-of-sale hardware and software is capable of accepting transactions. This will take considerable time, as will updating existing point-of-sale equipment. Like smart cards, the retail environment will suffer from the 'chicken and egg' phenomenon, as consumers will not like to adopt biometrics at the point of sale until retailers do, and vice-versa.

Of course to use biometrics for online shopping, each shopper must be able to submit a biometric sample, meaning they could require specialist equipment, such as a fingerprint sensor. The price for biometric devices is dropping rapidly, however, as production levels rise – for example a fingerprint-enabled mouse can cost well under US$75. Plus many new computers have microphones and cameras, or even built in fingerprint sensors.

However, while e-business might seem the obvious place for a biometric solution, it will not be easy to overcome the challenges involved. The failure of **ekey**, an Austrian company that was promising to run a highly ambitious e-business project across Europe, is a good case in point. It was to use biometrics in a fingerprint-based internet payment trial and had the backing of some major industry players, such as **Visa**, **Compaq and IBM**.

The project experienced some fairly major problems as Compaq and HP merged and as the lead investor pulled out. However, Roman Mandyczewsky, general manager at ekey told *Btt* that there were flaws in the company's business plan, including the fact that financial institutions were not particularly willing to pay for enhanced security measures. He also pointed out that it was debatable whether or not biometrics could reduce internet fraud significantly, as most internet fraud occurred initially in the physical world through stolen credit cards, rather than in the virtual world through compromised credit card details.

Two leading facts influenced the ekey project, according to Mandyczewsky – the predictions of massive growth in e-commerce and the perception that the internet is highly insecure. Both of these turned out to be exaggerated, leading to the eventual demise of the company business plans at the end of last year.

One company selling systems in the e-commerce arena is **Touchcredit**. Notably its product offering *BioAssure* recognises the fact that many consumers, banks or retailers (depending on how the system is operated) would not be prepared to pay for the hardware needed by consumers. Its system is therefore based on keystroke dynamics technology, which only requires a software programme to run on the consumer's machine, in order to recognise them via their distinct typing rhythm.

Monitoring staff

Away from the consumer side of the retail sector, biometrics can also be useful in the management of staff. This can involve physical access control, time and attendance monitoring, allowing access to cash registers or to enable special management functionality on cash registers (such as dealing with returned goods etc.).

One good example of biometrics being used for this purpose is at the retailer **Men's Warehouse**. The company has installed extremely sophisticated software which is aimed at making the shopping experience for men as quick and as painless as possible. Included in the software is a fingerprint system using **Key Source International** hardware, which allows managers to make returns or exchanges an extremely quick process. With the company's old system employees had to wade through several screens and passwords to handle returns, for example.

The system also helps the chain cut down on losses from employee theft and can monitor who is using the system at any particular time.

Money to be made?

There is clearly plenty of opportunity for the biometric industry to make inroads into the retail sector. This is occurring primarily in the cheque cashing sector at present, but in the longer term the use of biometrics as a payment option is increasingly likely.

A major question is whether biometric companies can actually make any money out of the retail sector. Simplifying matters, some companies, such as Indivos and BioPay charge on an installation and transaction fee basis (BioPay makes a monthly charge regardless of transaction levels), while others, such as BAC take a substantial fee up front, but then hand the database of customers over to the retailer, so eliminating ongoing transaction fees.

All these models have merit. The transaction fee model needs a large number of transactions to take place before really meaningful revenue can be achieved, but can be highly rewarding. The one-off fee is more predictable but limits the solution to one retailer, which may not be an attractive option in the longer term. The monthly service fee is also attractive due to its predictability for both the retailer and the vendor.

Whatever model proves most successful, it seems that vendors have so far been quite successful in selling the idea of biometrics to the retail world, but there is still a great deal more to be done.

Company	Telephone	Fax	Email
BAC	+1 512 246 3760	+1 512 246 3768	hrios@biometricaccess.com
Biocom	+1 310 305 3764	+1 310 577 0262	info@touchcredit.com
BioPay	+1 866 324 6729	—	trobinson@biopay.com
Datamax System Solutions	+1 561 994 1250	+1 561 997 6411	info@datamaxsys.com
Hypercom	+1 602 504 5000	+1 602 866 5380	—
IBG	+1 212 809 9491	+1 212 809 6197	tprout@biometricgroup.com
Solidus Networks	+1 415 882 1505	+1 415 882 1560	info@solidusnetworks.com
Touchcredit	+1 310 305 3764	+1 310 577 0262	info@touchcredit.com
Verifone	+1 770 754 3653	—	michelle_graff@verifone.com

A selection of companies operating in the biometric-enabled retail sector.