

## Banking and Financial Products Application

Fake debit cards, cash cards, and credit cards are a serious problem both for consumers and issuing banks.

A recent survey showed that many Japanese regional banks have suffered damage from counterfeit bank cards. But Japan is not alone in the fight against fake cards. Skimming is rapidly growing in virtually every major city in the United States, United Kingdom, Europe, Canada, and Latin America. It is especially rampant in Asia. It is estimated that the average skimmed credit card will generate some US\$2,000 in fraudulent charges before being detected and stopped. According to one report, skimming now ranks behind only lost and stolen credit cards as a contributor to fraud losses.

Stealing magnetic stripe information and customer PIN numbers ('skimming') is the biggest problem in bank fraud today. More recently, counterfeiters in Japan have tricked customers into giving away their personal information through email and fraudulent websites ('phishing'). Increasingly complicated skimming methods make it harder to address the problem with existing security measures.

### Existing solutions

Urged by the Japanese Bankers Association, member banks have taken steps to combat this problem. However, new technologies being considered still need to show reliability and effectiveness. One such technology is issuing ATM cards with chips and many Japanese banks are considering using these chips in their bank cards. However, even the complex chips used in game consoles such as Gameboy™ and Playstation™ are counterfeited so simple chips suitable for use with debit and credit cards will pose little problem for counterfeiters. Another method is to install automated teller machines with enhanced security features based on biometric identification. However biometric solutions face a number of problems as explained below.

### Bilcare Technologies' solution

Bilcare Technologies can provide bank cards with unique "fingerprints" - technology that we call Singular ID. Since the fingerprints are made using naturally occurring disorder, even we are unable to reproduce any fingerprint. Consequently any bank card that uses the fingerprint is effectively unforgeable. The production cost of tags is very low, and the readers are also inexpensive. The readers can be installed within existing ATMs and incorporated into electronic point of sale (EPOS) card readers. This will allow the Singular ID system to be introduced and used alongside the existing infrastructure in a seamless and cost effective transition.

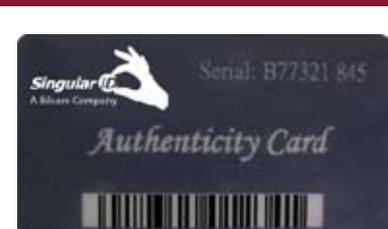
### Technology

Bilcare Technologies' patented and patent pending Singular ID solution provides a very flexible and secure system that can be retrofitted to existing ATMs and rolled out inexpensively as new bank cards are issued. Key components of the technology are:

**Unique Tags** can be embedded within the existing format of bank cards. Each individual tag has a "fingerprint" structure that confers it a unique



A scanning electron micrograph of Singular ID fingerprint technology. The fingerprint consists of micro- or nanoscale features embedded within a material. Each fingerprint produces its own unique signal and even we are unable to reproduce a fingerprint.



A demonstration swipe card containing a working invisible Singular ID fingerprint.

signature. Tags can be incorporated overtly or covertly into a wide range of materials including plastic.

**A database** that stores fingerprints together with the personal, banking and security information of card holders. The functionality of this can be incorporated into the existing banking database systems as an added module.

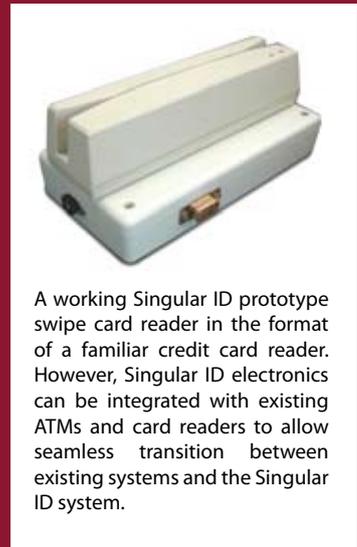
**Readers** that can be retrofitted to existing ATMs and rolled out in new credit card readers. These are designed to detect the fingerprints of tags embedded in cards and send the information over the same network as the existing infrastructure.

With the Singular ID system, debit cards can be authenticated not just by the conventional method of verifying a PIN number, but also by reading the unique fingerprint of the tag embedded in the card and then comparing it with stored information in the database.

While biometric identification systems such as vein pattern, iris and human fingerprint recognition could be viable solutions, they require entirely new infrastructure to be installed which will be costly and will be difficult to integrate seamlessly with existing ATM or card readers. Furthermore consumers tend to react negatively to any system that they believe may infringe on their privacy – this often makes biometric solutions difficult to implement.

### Summary

Singular ID tags can be integrated inexpensively into cash cards, debit cards and credit cards. These tags are practically impossible to fake. Singular ID readers can be integrated into existing ATMs and EPOS readers or rolled out with new readers as required. The algorithm matching routine and database requirements can easily be incorporated into the existing banking database network. Therefore, the Singular ID system provides banks with a reliable, cheap and secure solution to the growing problem of credit card fraud.



A working Singular ID prototype swipe card reader in the format of a familiar credit card reader. However, Singular ID electronics can be integrated with existing ATMs and card readers to allow seamless transition between existing systems and the Singular ID system.