FITEQ
FINANCIAL TECHNOLOGIES
Tiburon, CA 94920 Phone: (415) 435-4500

February 22, 2011
The Honorable Ben Bernanke,
Chairman
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, Northwest
Washington, DC 20551

FRS-2010-0379-0001
Docket ID: FRS-2010-0379

Introduction and Summary

The central question posed by the Board for comment is whether it should adopt a technology-specific standard or one that is non-specific with respect to interchange adjustments. We believe that neither is appropriate, and that instead the Board should adopt a performance standard, as other commenters have suggested (the Merchants Payments Coalition (MPC), for example), and as other regulatory agencies commonly do.

The weakness of a technology standard is the same weakness of any regulatory "command and control" design standard – it freezes technology and discourages innovation. A non-specific standard, on the other hand, demands too little and thus equally discourages innovation. In addition, under a non-specific standard it is impossible to monetize the costs to all parties to determine eligibility to receive an adjustment for fraud prevention expenses. A performance standard addresses the vulnerability of both extremes.

What should a performance standard look like? The Board has correctly identified through its own factual development that a PIN approach is a more effective fraud-prevention technique than signature debit. There is, additionally, the reality that in Europe and most other countries, routine counterfeiting has been reduced significantly by the adoption of Chip-and-Pin EMV (Europay, MasterCard Visa) technology.

There are, however, problems - at least in the short-term - with EMV (as noted in data provided by the Cambridge Computer Lab). Even when adopted, EMV does not defeat all fraud - for example, it was not able to stop the £725,000 “petrol station” fraud in the United Kingdom. In addition, the Payment Card Industry (PCI) report on Data Security Standards (DSS) in October of 2010 highlights the vulnerability of cardholder data in the clear from an EMV chip. Perhaps more importantly, EMV is expensive to implement (especially burdensome for merchants like gas stations), and has run into significant resistance within the U.S. historically. Hence, hackers move to jurisdictions which are slow in adoption, or to applications like “card-not-present” (CNP) sales (where the terminal upgrades are irrelevant and the issue is whether there is a better authentication system than the static card security number which itself can be compromised).

Are there other approaches that, for example, can provide (1) an EMV-level of security that does not require any change to existing magstripe terminalization and (2) a dynamic card security number that is generated per transaction and cannot be compromised by capturing the data on the magnetic stripe? If there were, a performance standard might tease out a solution that does not unfairly shift the cost of fraud prevention to the merchant from the issuer.

The answer is that there is at least one different approach that has been developed to preclude fraud. The technology is within the card itself, it can be used with the existing legacy of magstripe readers and it does not require - but is interoperable with EMV, Chip-and-Pin terminalization infrastructure. The technology can also develop dynamic card identification numbers for each new CNP transaction that cannot be re-used if captured by hackers.

The availability of this and similar approaches allows the Board to develop a performance standard that requires a minimum level of performance–such as the fraud level associated with PIN debit–and then grant a sliding fraud prevention adjustment to issuers for card technology they adopt that provides fraud prevention above the PIN level without imposing any terminalization costs on merchants. An allowance for fraud prevention should be no more than what is necessary for banks to recoup their net costs (their own costs minus any related costs imposed on other parties as a result of the prevention programs such as PCI changes or POS upgrades). There should be no allowance for fraud itself so as to avoid creating incentives to be less vigilant in eliminating fraud.

The specific suggestion by MPC, which we endorse, would allow the issuer an adjustment equal to that percentage of 1.2 cents per transaction (the issuer cost for PIN fraud prevention) attributable to the additional fraud prevention achieved by the issuer's "low fraud technology." If, for example, fraud losses are 50% lower from a new card technology than the PIN level (as determined by the Board), then the issuer would be granted a fraud prevention adjustment of 0.6 cents–which could be higher as the fraud reduction increases.

What kind of card technology is available? In the next section we will describe one approach, the key elements of which are already widely used in the payments system in connection with "contactless" payments (and which are also endorsed by the Smart Card Industry Alliance as described below). The National Retail Federation (NRF), the National Association of Convenience Stores (NACS), and the Petroleum Convenience Alliance for Technology Standards (PCATS) all have welcomed the development of FiTeq's solution as a low-fraud technology option for possible adoption under a performance standard.

A New Approach

We would therefore like to introduce the Board to a secure payment card technology which offers the best of *both the new EMV chip cards and a more secure existing magnetic stripe technology. Described in more detail below, this new battery-powered card technology can provide cardholders and merchants a higher level of security whether a transaction is made using a chip card reader or a conventional magnetic stripe reader. Thus, while the new cards work at EMV readers, they also generate a transaction-specific code within the standard magnetic stripe data packet, which is readable by conventional magstripe POS card readers. In particular, the new cards contain Dynamic Authentication Code technology to prevent criminals from re-using card data pilfered through account data compromise (ADC), which can occur in EMV-compliant locations, as illustrated in the recent £725,000 "petrol station" fraud in the UK. Put another way, these cards will see improved performance in countries that have deployed EMV and can also enjoy the benefit of dynamic authentication in mag stripe readers when using their cards while traveling to the US or any other country where EMV has not been deployed.*

The immediate benefit for merchants would come from enhanced security leveraging EMV cryptology in the form of a new technology card readable by existing magnetic stripe terminals, thus avoiding the significant costs associated with a mandated transition to EMV POS terminals. Such mandated EMV transitions are typically accomplished by shifting liability from issuers to merchants, thus requiring expensive re-terminalization and IT changes. Tests over the past 10 years at Target and various merchants in the upper west side of NY failed to build cardholder or merchant demand. In addition, the total cost for the U.S. retail market is estimated to be as high as $30 billion, a significant deterrent to EMV adoption in the US so far.

Adopting the EMV-compatible technology would make a shift to EMV readers unnecessary. However, even if EMV were mandated in the U.S., the full transition is estimated to take between 10 and 15 years (and even then the new technology could provide additional security by precluding breaches such as the UK “petrol station” fraud). Absent wide-spread adoption of the new technology, the U.S. - with its enormous legacy network of magstripe POS readers as well as magstripe cards - would be increasingly vulnerable to fraud during this time.

A workable example of the new dynamic card technology has been developed by FiTeq. FiTeq did not invent EMV chip card technology, but it has discovered how to make it better. FiTeq uses the power of EMV cryptography inside a battery-powered card to present secure magnetic stripe data to conventional magnetic stripe readers. Inside the card, a MasterCard or Visa certified EMV chip populates a transactions-specific FiTeq Unique Code into the conventional magnetic stripe data packet. The issuer’s Authorization system authenticates that FiTeq Unique Code before making its decision to accept/deny the transaction. Even if organized crime, terrorists or ingenious hackers compromise the FiTeq Unique Code-enabled transaction data, they cannot reuse that static data in any subsequent transaction. This is because the issuer authorization system requires for each new transaction a new FiTeq Unique Code number which is generated each time the card is swiped.

FiTeq was founded to develop innovative ways to reduce payment card fraud while working within the existing legacy system of magnetic stripe terminals and transaction networks. FiTeq understands that smart cards would be adopted slowly, if at all in this country, which gave rise to a compelling need to make the legacy system itself more secure. Prior security approaches, e.g. card holograms or printed security codes were easily circumvented, as they were static and unchanging, hence transparent to fraudsters. Re-terminalization is unnecessary with FiTeq’s solution because secure data is received from the card using the existing legacy magstripe POS terminal infrastructure and is contained within the traditional magnetic stripe data packet format.

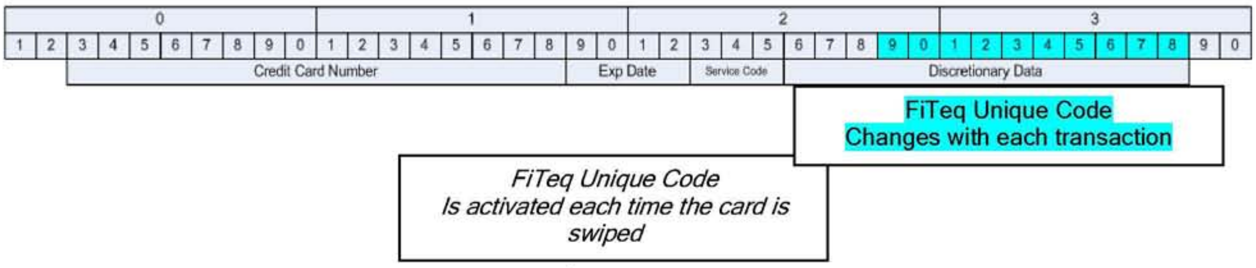
To repeat, the FiTeq solution is dynamic. It creates an authentication code that is unique to each transaction. Because counterfeit card data (captured by a skimmer or Account Data Compromise/ADC) lacks the ability to generate this transaction-specific code, the issuing bank knows to reject the fraudulent transaction. FiTeq’s fraud prevention technology is also designed to be adaptable to a variety of terminal types including Radio Frequency/contactless and Near Field communication (NFC) cell phones. Indeed, the Board can reduce concerns about fraud related to ADC with the knowledge that FiTeq's solution licensed the technology that was secure enough to be adopted by AmEx's ExpressPay, Discover's Zip, MC PayPass and Visa payWave to preclude reuse of contactless card data.

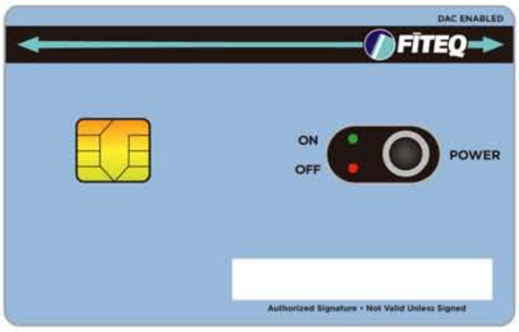
Because it does not require full reterminalization, issuers are not forced to wholesale replacement of cards. Rather, FiTeq's solution is suggested to be deployed among the top quartile or quintile of the issuer's portfolio, those accounts with high credit lines and frequent transactions which are most vulnerable when compromised by fraudsters.

In addition, because FiTeq cards can change the magnetic stripe information with each transaction, FiTeq can also offer significant upside to all stakeholders in payment cards. Issuers and merchants can benefit from interactive cards that offer a variety of payment cards all-on-one plastic. Issuers and merchants can offer customized Customer Relationship Management (CRM) programs with interactivity among all parties at the point of sale. Although the security benefits provide an immediate ROI to the merchant and bank, these interactive technologies offer significant additional value to all stakeholders.

FiTeq's solution is in two parts:

1. The first is a battery powered electronic card with a core technology that energizes the magnetic stripe so it changes with each transaction, FiTeq's Energizer Stripe. An EMV smart chip encrypts a FiTeq Unique Code within the conventional magnetic stripe data packet, leveraging the years of cryptography built into EMV smart chips, but ensuring that a higher level of security is readable by legacy magnetic stripe terminals, which are still the most ubiquitous terminal in the payments market.





2. The second part is the FiTeq Vault Authentication Software module that resides on the issuer's authorization platform. With a single API call, the issuer can detect and deny a counterfeit card and approve the genuine card issued by the bank because it has the next correct FiTeq Unique Code embedded in the Energizer Stripe. Before making a decision whether to accept or deny the transaction, the issuing bank can first authenticate that the card is the genuine card issued by the bank because it will have the same key to ensure the correct FiTeq Unique Code is in the magnetic stripe data packet.

- Thus, if a FiTeq Energizer Stripe card was compromised in an ADC, the data could not be re-used by a fraudster because each FiTeq Unique Code is good for one and only one transaction.
- For US debit cardholders traveling abroad, the EMV approved chip can enable an EMV approved payment applet.
- For international issuers that seek a higher level of security when cardholders travel to the US, those cards can be used in magnetic stripe terminals with the FiTeq Unique Code. In the event of ADC, the chip card would not have to be replaced. If skimmed, the counterfeiter would not have the ability to generate the next Unique Code, so it would be stopped cold.

It is worth noting that as a result of FiTeq's choice to license the dynamic authentication code (DAC) technology, already in use by over 100 million cards in connection with contactless payments, the Smart Card Industry Alliance White Paper endorses US contactless dynamic authentication security as an ideal means of containing fraud. Their white paper lays out the two important advantages: 1. It renders stolen cardholder data on counterfeit plastic useless to criminals attempting transactions in retail locations. 2. The existing U.S. payments infrastructure can process such transactions today, as it does for contactless payment. Thus, the Smart Card Alliance is

> . . .proposing another option for the U.S. payments market that **has clear benefits over both EMV "chip and PIN" and end-to-end encryption: Use contactless chip cards, include a dynamic cryptogram with each transaction and authorize transactions online.** The U.S. payments industry supports contactless payment transactions with three-digit, online dynamic cryptograms today.[9] Combining this with velocity checking in all credit and debit card processing would be **a very effective barrier to counterfeit card fraud.** The **cryptogram itself is a type of digital signature that works in conjunction with traditional magnetic stripe data.** The cryptogram is a value based on specific inputs for an individual card and transaction that makes each transaction unique. Since only the chip card itself can create a valid cryptogram, the authorizing host can confirm that the actual card is present. In addition, the **cryptogram is generated using secret keys inside the chip card, so key management is not required for merchants. The card issuer controls key management entirely.** [emphasis added]

In addition, FiTeq's technology has already conformed to the payment networks infrastructure and passed ISO and security standards.

Conclusion

Because of the proven track record of the technology in contactless that is now available for magnetic stripe terminals, the Board can specify as a minimum the fraud reduction and cost savings that the existing technology can produce, and give an extra margin for improvements that no doubt will materialize as suggested by the Merchants Payments Coalition (MPC). If there is a cheaper card technology that can achieve today more than FiTeq does, then the Board's performance standard would lead to adoption of that approach over FiTeq's. On the other hand, however, the Board should not be so standardless as not to incentivize at least the performance and cost savings of approaches that are already proven today.

A recent report in the Washington Post (February 17, 2011, A13) cites banking industry contentions that the Board's proposed interchange fee "is not enough to recoup the full cost of the necessary computer infrastructure or provide security and fraud protection." Implementing FiTeq's solution could go a very long way in containing, at low cost, at least the fraud and security expense faced by the industry.