QwyitCard™ Summary

You've probably received new smart chip credit cards over the last few years to replace your old ones. These are called EMV Chip and Signature (or the less used in the US, Chip and PIN) 'smart cards', introduced by Europay, Mastercard and Visa. These are for fraud reduction introducing two main characteristics: they can deliver a unique identifier for each transaction along w/the static card number providing more security, and they store and contain encrypted data making the cards difficult to counterfeit.

The reason credit card fraud needs to be reduced is because it's over $3*billion* in US retail merchant market losses (in 2015!) – and rising! Unfortunately, those EMV chip cards are costing $3*billion in* implementation – which is only about 60% complete – and the estimates for a total EMV solution rollout are…*$8-12BILLION!* And the fraud rate is only down 58% from March 2016 to March 2017.

This total *$15Billion* problem is completely unnecessary. Twenty years ago, a Qwyit® technology solution was proposed and presented that completely eliminates over 95% of the fraud scenarios – and costs literally *nothing to implement!* Our solution is called QwyitCard™, and it can be delivered using legacy swipe cards and their existing 'dumb' readers after a quick firmware update.

The exact same fraud reduction properties that are inherent in the $15Billion EMV cards are in QwyitCard™ - using superior techniques that actually work to solve the problem, whereas the new chip cards are *already broken*:

> *According to Aite's 2016 Global Consumer Card Fraud report, it is safe to assume that all users have been compromised. Whether you use a card with a magnetic stripe or a more secure chip-and-PIN card doesn't matter — if you have a card, its information has probably been stolen. Now that criminals have developed a method to actually clone the cards, that starts to look like a very serious financial threat. – from Kaspersky Daily, 3/9/2018*

The fraud reduction properties of QwyitCard™ aren't original anymore (albeit, they *were* when introduced 20 years ago): a unique transaction number, and some kind of new method providing replication deterrence. In addition to the catastrophic EMV chip cards, there are several smart phone apps that 'do the same thing'; some of which handle payment processing along with presentation. All of these – and the reason that none of them have replaced 'The Credit Card' – suffer from two fatal flaws:

- The solutions are *secondary*; i.e., they require having a *credit card in the first place*
- The solutions don't add any security, even though they claim to; i.e., their methods introduce an underlying pyramid of *new attack points while (supposedly) fixing the original ones*

Instinctively, people understand both of these are just another layer of vulnerability – the Credit Card is still king, even though the new EMV cards are broken. This means that any new solution proposing the required fraud-reduction properties possess the following *system properties* in order to surmount proliferation obstacles (unless it is being driven/mandated by the credit Issuers themselves – such as their EMV):

- Whatever infrastructure update is required, it must be simple, zero/low cost, and performed simultaneously with any Card improvements (preferably *before* new cards are put in use)
    - Realistically, this can only be a simple firmware update to existing card readers
        - This means a small-kit SDK code/instructions accompanying suggested 'API' connectivity to the widest possible known/used readers in order to immediately begin processing new cards
- Whatever backend processing is required, it must be simple, low/zero cost, and put in place simultaneously with any Card improvements (preferably *before* new cards are put in use)
    - Same type of SDK/API insertion kit, modeled for existing backend services
    - The insertion must have *minimal impact* on current processes
        - Realistically, this would just be at the 'messaging ends' – the 'send' and 'receive'; then all existing prep (at the reader, which has the above simple compatible SKD/API kit already inserted) and processing (the backend) can proceed normally
- Whatever Card improvements are proposed, credit card users must instinctively know how to participate; i.e., whatever is 'in addition to' simple swiping must immediately be recognizable/understandable

QwyitCard™ meets all of these requirements (*and exceeds them – below in italics*):

1. An improved Credit Card – *NOT a secondary implementation*
    a. Meets all of the fraud-reduction properties
        i. Unique transaction data
            1. *Actually mixed into the Credit Card Number presentation*
        ii. Card is PIN-protected against replication/duplication
            1. *PIN can easily be set at exponential increase over current*
        iii. Customer Verification Value (CVV) is improved (a QwyitCard™ Proof Key), adjustable to Issuer-required risk
            1. *Actually has lasting protection even after partial discovery*
        iv. All properties are based on sound, provable mathematics
            1. *Underdetermined equations – unbreakable/unsolvable over the entire life-cycle use of all cards for all users*
            2. *Cards cannot be skimmed, shimmed, scammed or otherwise replicated using card data and/or intercepted transmissions (even if open, unencrypted)*
    b. Improvements have no Card impacts
        i. Zero cost
        ii. Located on unused, existing card structure
    c. Infrastructure processing has no impacts
        i. Less than 100 Milliseconds at reader
            1. *Improved Customer experience – speed, convenience, exactly compatible with existing process*
        ii. Less than 100 Milliseconds at payment processor
            1. *No additional approval time*
2. The SDK S/W for implementing QwyitCard™ is already written in C/C++/Java
    a. Less than 5K in code space
    b. *Firmware push performed easily*

i. *At reader, at Issuer/processor*

3. Additionally, Qwyit® has tools for unbreakable security of transaction communications and data storage security (QwyitTalk™/QwyitStore™) as well as a complete upgrade of the entire credit transaction process called QwyitCash™ that eliminates the card and the reader entirely!
    a. *All of these processes are provably secure: Unbreakable*

The summary benefits of QwyitCard™:

A substantially improved Card, process, implementation, economics, experience
With considered, capable future realizations

Why on earth are we spending ***$15BILLION*** on a faulty solution?!