A Solution to the Mobile Wallet Conundrum
Introduction: A new approach is needed to make the Mobile Wallet mainstream

More people than ever are using smartphones to place and take phone calls, write, send and receive emails, read the news, check bank accounts, take photos, and browse friend updates on social media. Yet, the use of mobile wallets and payments has, thus far, failed to be adopted at any appreciable level despite the fact that these applications seem naturally suited to these devices carried around by half of all adult Americans.

There are two primary reasons for this lack of adoption:

- Existing payment methods, such as credit cards, have proven to be ill suited for storing on mobile devices
- To date, mobile wallet applications have proven to be less user friendly than the status quo (credit and debit cards) – this has been a major roadblock to adoption

Cortex MCP has developed a new technology platform from the ground up to address the challenges, and opportunities, of the mobile ecosystem. It considers the need for both payments and identification to deliver a complete wallet solution that is more secure and more convenient than alternatives (including physical cards). It also incorporates an offer platform that delivers value to the consumer and merchant above and beyond what is available in the market today.

Cortex MCP is not offering the platform directly to consumers. Instead, the platform is an enterprise offering designed to be leveraged by banks, credit card companies, and other e-wallet providers so that they can provide a superior mobile wallet solution for their customers. The platform has been designed with backend payment, offer, and identification services accessible via APIs to power Cortex MCP partner iOS and Android mobile wallet applications. And it is designed to work with existing payment methods and infrastructures.

The first section of this whitepaper will review past attempts at mobile wallet implementations and highlight their shortcomings. The paper will then introduce the major components of the Cortex MCP mobile wallet platform, including the RCD™ payment method, Pre-Commerce™ / Intent-to-Spend (ITS) Analytics™ for offers, and OVER File™ identification.
Background: Why aren’t consumers using mobile wallets today?

To date, there have been two main approaches to bringing mobile commerce to mainstream use. The first involved the use of Near Field Communications (NFC) and what is known as a “Secure Element” chip (or SE) embedded in a physical device. The second is leveraging cloud-based mobile payments technologies.

Near Field Communications using the on-device Secure Element

The idea behind this method is to store the user’s credit card track data on the phone, inside the SE. The SE is a special chip purposefully designed to store credit card data in a secure way. It is separated from the rest of the phone’s hardware and special procedures are required to access it so as to prevent hacking. This security is necessary because if hackers gain access to the SE data, they could not only make fraudulent purchases but even create fake credit cards. An example of an early SE implementation was the Google Wallet app. The idea was that users could load their credit card into their phones and simply wave it at a POS terminal, leveraging NFC, to pay for their items.

The mobile commerce initiatives that have launched around the SE approach have failed to achieve mainstream use. There have been a lot of bureaucratic and political issues in accessing the SE chip (e.g., the widely publicized disagreement between Google and Verizon which led to Verizon shutting down the Google Wallet app on their network). In addition, the special hardware required has also proved to be a major barrier. Apple has never built the SE into any iPhone model (although they do have a patent on a secure enclave that is somewhat similar). Even in the Android space, despite Google’s early endorsement of the technology, most phones do not include the SE.

Cloud-based mobile payments

The second approach to mobile commerce involves storing a user’s payment data in the cloud instead of on the mobile device. This eliminates the need for the SE as the credit card information is not being stored on the physical device.

Several variants of cloud-based mobile payments are being offered in the market today. Three of the more prevalent include the “check-in” method, the “push” method, and “Host Card Emulation” (HCE).
Check-in method

The check-in method works by having consumers use their smartphones to “check-in” to a retail location and authorize payment. The user “checks-in” on their mobile device at the time of purchase or before arrival at a store. Upon checking in, the user’s photo appears on the POS screen (requiring a hardware upgrade). The consumer then informs the merchant that they want to pay using the check-in method. From there, the merchant checks for the customer’s photo and authorizes the transaction. An alert is then pushed to the user’s device confirming the purchase.

The check-in method requires substantial changes in both user and merchant behavior. It also requires that merchants install a special device or upgrade their existing POS systems so that they’re capable of displaying these photos – this can be costly. The method has also encountered practical hurdles. For example, while the photo matching method works well for a business such as a small coffee shop, it can be more time consuming at a large discount store where many customers may be waiting in check-out (check-in?) lines during peak shopping hours.
**Push method**

Other vendors have implemented a “push” method whereby upon checkout, the merchant first requests a token from the mobile payment network in the cloud for that specific purchase and presents it as a QR code. The consumer then scans this QR code with their phone and transmits this code along with the authorization back to the cloud-based payment network. At this point, the network then matches the two codes and transmits the final authorization to the merchant, completing the checkout process. The primary issues with this method are the specialized, expensive equipment that needs to be installed at the merchant, and the numerous changes that it requires in merchant and consumer behavior – not to mention that both the POS and consumer devices have to have fast data connections to work.
• **HCE method**

In the meantime, Google has changed course from storing the credit card data on the SE and has introduced support for the new **HCE method** in their latest Android OS update. HCE works by storing the credit card in the cloud and pulling the credit card information to the phone, where it can then be transmitted using NFC. It does not require a SE on the device. (In fact, Google’s latest phone, the Nexus 5, does not even include a SE.) Yet, the security issue still remains, as the full credit card track data must be transmitted to the user’s device at the time of purchase. And so care must be taken to ensure this data is not “sniffed” or compromised by hackers.

All of these cloud-based approaches suffer from their dependency on the user having an active network connection at the point-of-purchase. What if the user has no network connectivity or cell coverage in the area where he/she would like to pay? In these instances, cloud-based methods fail the “lowest common denominator” test, and the user would need to bring a physical credit card as a backup payment method. But even if there is network connectivity, the user still must authenticate and authorize that purchase over the network. And despite today’s higher cellular network speeds, this still takes time – certainly more time than simply taking an actual credit card out of a leather wallet.

A third approach, on-device **tokenization**, has been introduced as an alternative to the SE and cloud-based methods. Tokenization works by having the user request a “token” that is then placed on to the user’s device. This token represents an amount of money pre-authorized by the user. Upon check-out, the user presents the token for payment via NFC or QR code. The merchant then scans the token and checks its legitimacy. It requires some changes for the merchant, as they have to purchase
new hardware and adopt a new process for authenticating tokens for payment. It also has security concerns for the user because once the token is on the device it needs to be protected from hackers less someone, other than the user, use it.

One final point: to truly replace a consumer’s wallet, mobile payments are not the only requirement. Identification is important too. After all, most everyone carries a driver’s license or identification card in their wallet. In addition, consumers often carry other credentials such as medical cards, store loyalty cards, and health club membership cards. For a mobile wallet to replace the physical wallet, it needs to support these identification requirements as well. A mobile wallet platform that provides comprehensive support for both mobile payments and identification verification has yet to be introduced.

Consumers are not using mobile wallets broadly today for one simple reason: the offerings don’t compete with the simplicity and convenience of paying with a credit or debit card. Mobile payment solutions either require the consumer and merchant to purchase special hardware or to change their behavior – all of which is very inconvenient. In addition, neglecting support for other credentials, something as obvious as a driver’s license, keeps mobile wallet adoption further at bay.
A new approach is needed: Introducing the Cortex MCP - Mobile Wallet Platform

The sections below detail the three key components to Cortex’s mobile wallet platform:

- The RCD™ payment method
- Pre-Commerce™ / ITS analytics™ for offers and loyalty
- OVER File™ identification.

Each of these components is based on patented technology that has been developed by Cortex over the course of several years. And all are designed to integrate and interact seamlessly with today’s commerce and identification systems.

RCD™ Payment Method

Reducing Currency Denomination (RCD) is a new payment instrument specifically designed for mobile devices. It’s an alphanumeric string containing a user-defined, four character PIN corresponding to a limited amount of money. The RCD requires no special hardware and is stored on the user’s device. It can be passed at the point-of-sale via bar code, QR code or NFC and transmitted via existing rails used for credit card transactions.
The RCD is secure:

- The RCD is always stored in an incomplete state, without the user-defined PIN. The user supplies the PIN at the time of the transaction (in a fashion similar to a debit card purchase). So even if someone illicitly gains access to a user’s phone, they’ll be unable to purchase anything without knowing the PIN.

- In addition, each RCD is unique to the user’s device on which it was created and is unusable on any other device. This way if hackers somehow gain access to both the RCD and PIN, they would be unable to use it without having the user’s actual phone. This is very different from and much more secure than the tokenization method.

- The name Reducing Currency Denomination comes from the fact that from the time a RCD is created, its value always decreases. Instead of adding money to an existing RCD, a new RCD is created with the remaining balance transferred from the old RCD to the new one. In this way, liability is always limited to the present amount set by the user. This is very different than a credit card where the liability can be as high as a consumer’s credit limit, often in the thousands or tens of thousands of dollars.

- The RCD offers additional control measures. For example, the user can restrict a RCD to certain retailers, product categories, or geographies. The user can also restrict the amount of money that can be spent for any single purchase and even the number of purchases per day. These features are particularly useful to parents who can provide RCDs to their children with more control over spending (e.g., allowing the purchase of food but not a video game).
The RCD is convenient and easy to use:

- Because of the security measures cited above, no SE is required to store the RCD on the user's phone. Therefore, RCD supports all smartphones: Android, iPhone, and Windows-based devices.
- Because the RCD is stored on the phone, users are able to use it instantly – faster than the time it would take to remove a credit card from their wallet. The user need only enter a four character PIN to pay. In this sense, paying with a RCD is very similar to paying with a debit card, ensuring that it will be familiar to users and easy to adopt.
- The RCD is passed via bar code / QR code or NFC at the point-of-sale. There are two options for supporting this pass-through at the merchant:
  - The RCD can be passed over the existing rails leveraged by credit cards using a unique, IP-protected methodology, requiring zero (for NFC) or minimal (for QR code) changes to the merchant’s POS system. Once the RCD leaves the POS, it is then routed via the processing network to the Cortex MCP backend which would either approve or reject the purchase and trigger the appropriate accounting function (i.e., a payment or refund).
  - Alternatively, the Cortex MCP APIs can be integrated into the POS terminal (mobile or traditional) such that the RCD would be routed directly to the Cortex MCP backend, initiating the approval process described earlier. The POS systems that can be supported most rapidly in this manner are Android and iOS tablet-based systems. This integration also supports features related to the Pre-Commerce / ITS Analytics for Offers module, described in the next section.
- The RCD can be funded via ACH, credit card, debit card, and other methods. It supports both limited pre-authorized amounts as well as pre-funded scenarios depending on business requirements and is compatible with all existing payment methods.

The most critical aspects of the RCD are its support for all of today’s smartphones and its familiarity to users in that paying with a RCD is very similar to paying with a debit card. The RCD is the first mobile payment method to meet these requirements and is a breakthrough in terms of powering mobile commerce.

Pre-commerce™/ITS analytics™ for offers and loyalty

Cortex’s ITS analytics module is an extension to the RCD payment mechanism and enables merchants to target offers to users who will be creating RCDs targeted to specific purchases. For example, imagine a user who creates an RCD to purchase a new TV with an amount of $1,000. Using Cortex’s ITS analytics, a nearby merchant nearby can push an offer to that consumer for a TV within his/her price limit. ITS creates a new offer platform tied directly to a consumer’s intent to spend for specific items. This opens up a powerful avenue for merchants to expand sales and provides them with a critical incentive to accept the RCD payment method in their stores.
The primary differentiator of ITS vs. existing “daily deal” offer systems is that consumers can be assured that any offer they receive will be directly related to an item that they want to buy. For the merchants, they’ll know that any consumer who receives their offer will absolutely be interested in it as they’ve already earmarked money for that type of item. Above and beyond the convenience and security factors inherent in the RCD payment method, it is the ITS offer platform that will drive consumer and merchant adoption.

**OVER File identification**

People use their wallet for more than storing cash and credit cards. As discussed earlier, a wallet also stores various forms of ID: a driver’s license, state ID cards, passport cards, store loyalty cards, membership cards, etc. In order to “leave the leather” at home, consumers will need to be able to leverage their mobile wallet for the purpose of identification. Cortex’s answer to this is the OVER File – an identification method that is highly secure and leverages much of the same technology as the RCD described above.

Its components include:

- **OVER File Storage** — This component stores and validates all OVER Files delivered to the user’s device. Each OVER File is unique to the user and device preventing its use or manipulation even if a hacker somehow gains access to the device or file. To show a given OVER File, the user simply enters a four-character PIN code and the OVER File will display it on their smartphone screen, along with a QR code that can be scanned by a third-party for verification purposes (see authentication application below). All OVER File storage functionality is bundled with the RCD payment functionality described earlier to enable a complete mobile wallet solution for the end user.

- **OVER File Authentication** — OVER File stands for “Officially Verifiable Electronic Representation.” The authentication application performs this verification; it is used by a third-party to verify a user’s OVER File identification credential. When a customer presents an OVER File identification, the third party (e.g., a bartender) would use the authentication application to scan that OVER File’s QR code. At this point, the authentication application would interface with the Cortex backend to validate that the OVER File credential (like a state ID card) the user is presenting is in fact valid and will return it with a green check mark. (In this scenario the state would be the issuing authority; please see the generation application below.) Conversely, if it is an invalid identification, the authentication application would alert the third party to that also.

- **OVER File Generation** — The generation application is used by an issuing authority to create OVER Files for their customers. For example, a state motor vehicle department could use the generation application to create a driver’s license OVER file for a state resident. This OVER file would contain any relevant photos and/or text. The generation application would create this OVER file and then deliver it to a user’s device. At that point, the storage application described above would validate it and store it securely along with the user’s other OVER files and RCDs.

In order to offer a complete mobile wallet solution to customers, identification must be supported. Cortex’s OVER File enables mobile identification for everything from driver’s licenses to state ID cards to store loyalty and club membership cards.
Cortex provides an enterprise-grade, wholly secure mobile wallet platform ready-to-go today

Starbucks is unique in that has found much success in leveraging their application for mobile payments. We believe the primary reason for this is the app is so easy to use, and their target market is relatively tech-savvy. Consumers simply start the app, scan the QR code, and get their coffee along with reward points. It’s clear that consumers are ready to adopt a mobile payment solution that is easy to use and works on their smartphones.

Cortex MCP provides a platform that lets its customers create a solution as easy as this. It supports all of the major smartphones being used today. Cortex’s RCD payment method mirrors a physical debit card in its convenience and ease of use. ITS analytics enables retailers to push offers to users who have demonstrated intent to spend delivering value to both parties. And the OVER File ensures a complete mobile wallet offering supporting identification and allows consumers to “leave the leather” at home.

Beyond these features, Cortex’s platform has been designed to be truly secure and scale to all sorts of purchases from cups of coffee to TVs to clothes to airplane tickets and much more.

Please visit www.cortexmcp.com to learn more about how the Cortex MCP platform can power a mobile wallet for your customers.