

# Trusted Service Manager: The Key to Accelerating Mobile Commerce

.....

As major players struggle to define their roles in the emerging mobile commerce ecosystem, how they enable one critical service will make all the difference between slow and rapid acceptance of mobile commerce by consumers.

.....

By Chris Cox, Vice President, Mobile Commerce Solutions

## Introduction

Imagine you are on your way to work, and you stop somewhere for coffee and a doughnut. Normally you would reach for your wallet and pay in cash. Or maybe you are buying coffee and doughnuts for the entire office and you want to put it on the company card. Again you reach for your wallet.

But today is different, because today you are not carrying a wallet. Instead, you have a commerce-enabled mobile phone. You reach for your phone and pass it near a contactless reader at the checkout. Your contactless transaction is complete in a fraction of the time it takes to make a traditional card or cash purchase.

Nearly everyone has a phone in his or her pocket, but before consumers can use their mobile phones to make purchases, those phones need a few enhancements that will transform them into electronic wallets. Turning a mobile device into an electronic wallet involves adding these components to the device:

- **NFC (Near Field Communication) chip:** NFC chips enable mobile devices to send account information to contactless payment readers at customer check-outs and other points of sale. These NFC chips can also read information stored in contactless-enabled tags placed on objects such as advertising collateral and consumer products
- **Secure element:** The secure element is a smart card module (USIM, embedded secure element or separate secure element like a secure SD memory card) used for storing and accessing applications and data in a secure manner
- **Electronic wallet application:** Mobile phones also need to have a user interface (UI) that allows a user to manage accounts and initiate contactless payments. These UI applications turn a mobile phone into something like a wallet full of cards because a mobile phone can contain many “cards” (credit, debit, prepaid gift card, other special stored-value accounts, public transit tickets and merchant-specific loyalty cards, just to name a few). The electronic wallet allows users to select the right card or application when making a purchase. Some mobile handsets being delivered today come with electronic wallet applications already installed
- **Personalized account information:** In the same way that a credit card only works only after personalized account information is put onto the magnetic strip and embossed on the front of the card, a commerce-enabled mobile phone is just a phone until it is loaded with personal account information

NFC-equipped phones are beginning to appear in the market today, and there are a number of wallet applications available, many offered by banks and independent mobile account management service providers. These options are discussed in more detail in other papers we've written covering mobile commerce (see a list of additional readings at the end of this paper).

However, before a consumer can buy something with his or her phone, the device must be "personalized" with appropriate payment application and account information. In some ways, this is similar to the process of personalizing or provisioning a plastic credit or debit card.

When you receive a credit or debit card, the card comes with your personal account information already imprinted on the magnetic strip or stored on an embedded chip, and your name and account number embossed on the front of the card. There are a few companies, like First Data, that provide provisioning services to card issuers. These services involve storing personal account information in accordance with Payment Card Industry Data Security Standards (PCI DSS), and transmitting that data during the card-issuing process. First Data performs this provisioning service today and has more than 700 million credit and debit accounts on file, which represents about half of all active accounts worldwide.

In the case of credit and debit cards, there is one provisioning process for each card. If you open your wallet and look at the cards you have, each one represents a separate provisioning process involving different financial or merchant entities. Companies that offer provisioning services typically maintain contractual relationships with many of these entities. For instance, First Data maintains relationships with a very large number of banks all over the world as well as all the major card associations. These relationships enable First Data to collect the essential personal account information needed for the provisioning process.

Provisioning a mobile NFC phone with personal account information is fundamentally different from card provisioning in two important ways:

- A commerce-enabled phone can contain many accounts. These can be credit accounts, debit accounts, merchant-specific accounts, transit pass accounts, loyalty accounts and others. Each of these accounts can come with its own personal identity, financial and security information. Putting these accounts into one mobile device brings together account information from many different business entities, some of which could even be competitors
- The only practical way to get personal account information into an individual's phone is through the mobile operator's wireless network. Account information is transmitted to the mobile phone by a process called over-the-air (OTA) provisioning. This transmission can be difficult to accomplish without the active cooperation of mobile network operators

There have been a number of pilot programs to test the viability of mobile commerce in typical consumer scenarios. The recent Bay Area Rapid Transit (BART) pilot in which 230 NFC payment-enabled phones were given to BART commuters is a good example. Those NFC phones were equipped with two accounts—one for purchasing BART tickets, and the other for purchasing meals at local Jack-in-the-Box restaurants. Like most mobile payment pilot programs, the phones were preconfigured with account information and then distributed for use by consumers participating in the study.

However, in the real world of mobile commerce, phones might not come preconfigured with account information. Furthermore, consumers will want the flexibility of adding new accounts to their phones in the same way they might want to sign up for a new payment card or a merchant loyalty account.

Clearly, a working mobile commerce solution depends on transparent systems for getting new or updated account information into the phone in a dynamic way. So, how will account information get inside all those mobile devices? This is an essential question that will help define the topography of the emerging mobile commerce ecosystem. The answer involves new mobile commerce inspired business relationships and a new kind of provisioning role called Trusted Service Manager (TSM).

## Trusted Service Manager – Provisioning in the Mobile Commerce Ecosystem

The concept of the TSM was initially introduced in 2007 by the Global System for Mobile Communications Association (GSM) to facilitate adoption of NFC services. The GSM is a trade association representing more than 750 GSM operators in countries and territories all over the world. TSM addresses the biggest challenge to realizing simple, transparent mobile payments within the mobile commerce ecosystem: bringing multi-account services to different mobile NFC devices accessed through a variety of proprietary networks.

A key element of the TSM role as envisioned by the GSMA is that it is an independent entity serving mobile network operators (MNOs) and any account-issuing entities such as banks, card associations, transit authorities, merchants and marketing companies, to name a few potential service providers. An independent TSM is key to the provisioning of applications to NFC-enabled phones such that they have the broadest possible purchasing power for the consumer.

For instance, it's conceivable that a bank working in conjunction with one of the major card associations could issue a phone through a major mobile network operator that is essentially a card association-branded phone. The card association or the bank might provide the TSM services for that one device. Such a partnership might resist adding merchant-specific prepaid accounts to those phones, because these accounts represent ways for consumers to make purchases without using the card association's payment network. While the card association might think this is a good strategy for its own interests, it actually limits the commerce potential of those phones by excluding accounts that make it easier for consumers to make their buying decisions. Those phones, then, become less valuable to the entire mobile commerce ecosystem. They will be used for fewer transactions than might otherwise be the case, which in turn also makes them less valuable as a channel for individualized marketing messages targeted to the consumers who carry them.

We will talk more later in this paper about the pitfalls of this more restrictive approach to the TSM role. The key point here is that an independent TSM is in a position to service mobile NFC devices with many accounts from many different service providers across many carriers and payment networks, and this is what will maximize the value of NFC-enabled mobile phones as a channel for not only consumer purchases, but also targeted marketing.

The core function of the TSM is to securely distribute, provision and manage the life cycle of NFC applications to the customer base of mobile network operators on behalf of service providers. But the TSM role is much broader than providing only the technical capability to provision and personalize NFC applications over the air. The TSM manages contractual relationships between many mobile network operators and many service providers. And the TSM provides many supporting business services, including customer service, data center hosting and quality assurance.



Critically, the TSM is the one entity in the mobile commerce ecosystem who has a view of the intersection of the customer base of the mobile network operators and the service providers. This view enables the TSM to provide customer support from both the MNO perspective and the service provider perspective and enables the management of customer life-cycle events such as exchanged, damaged, lost or stolen handsets (and associated impact on service provider accounts previously provisioned). Related to this is the TSM's responsibility for managing the life cycles of NFC applications, electronic wallet applications and mobile handsets/secure elements.

As mentioned earlier, the process for provisioning mobile NFC phones is far more complex than provisioning traditional cards. In most cases, credit or debit card provisioning is a service delivered by a neutral third party, such as First Data, which must obey strict rules governing the secure handling of plastics and of personal/financial information to prevent fraud. Traditional credit and debit cards are provisioned prior to being issued. Customers sign up for cards through a bank or other entity. When it's time to issue the card to an approved applicant, the issuing bank downloads personal account information from a service provider (such as First Data) that manages this data. The service provider puts the individual's personal information onto the card by embossing the name and card number and encoding account data to the magnetic strip.

But provisioning a mobile device is more complex for a couple of reasons:

- **Phones handle multiple accounts—not just one:** All this account information needs to be in a secure element (smart card chip) in the phone and associated with an individual's personal and unique authentication data
- **Consumers need to be able to manage accounts in real time:** Users must be able to directly manage their applications, adding or deleting them at will. This means the account activity that users initiate must also be "serviced" by the TSM on a 24/7 basis
- **Provisioning needs to be done over the air (OTA) and in real time:** With OTA provisioning, a user doesn't have to go to a store or a service center to have NFC applications installed or to add personalization data. For example, users can search a repository of approved NFC applications using their phone (after they are authenticated), and choose to download the applications they want. All of these OTA updates must occur over mobile carrier networks. This means that whoever provisions to NFC phones also needs to have strong relationships with multiple carriers

## Why is a TSM Necessary?

You may wonder why you can download applications like games and other utilities over the air to your mobile phone today, without the need for a new business entity like the TSM. Why is the TSM required at all? There are a few different reasons. The first and most important is that any application that requires your personal information (e.g., a credit, debit or other payment application) requires special handling. The application and your personal information must be stored in the handset's secure element and not in the standard handset memory. The technology required to provision and manage applications and personal data on the secure element is different than the technology required to download games and other non-personalized utilities. Especially in a world where applications from multiple competing entities could end up on the same secure element, the TSM plays a key role in restricting access to applications and data to only those with permission to access it.

Also, a payment application and the associated personal data are hosted by a financial institution or third-party processor in a secure data environment that conforms to payment industry security protocols. The TSM plays a key role in securely interfacing to these host systems and ensuring that all required secure data-handling processes are in place. A core component of this process is security key management, which is not necessarily required for games and other non-personalized utilities.

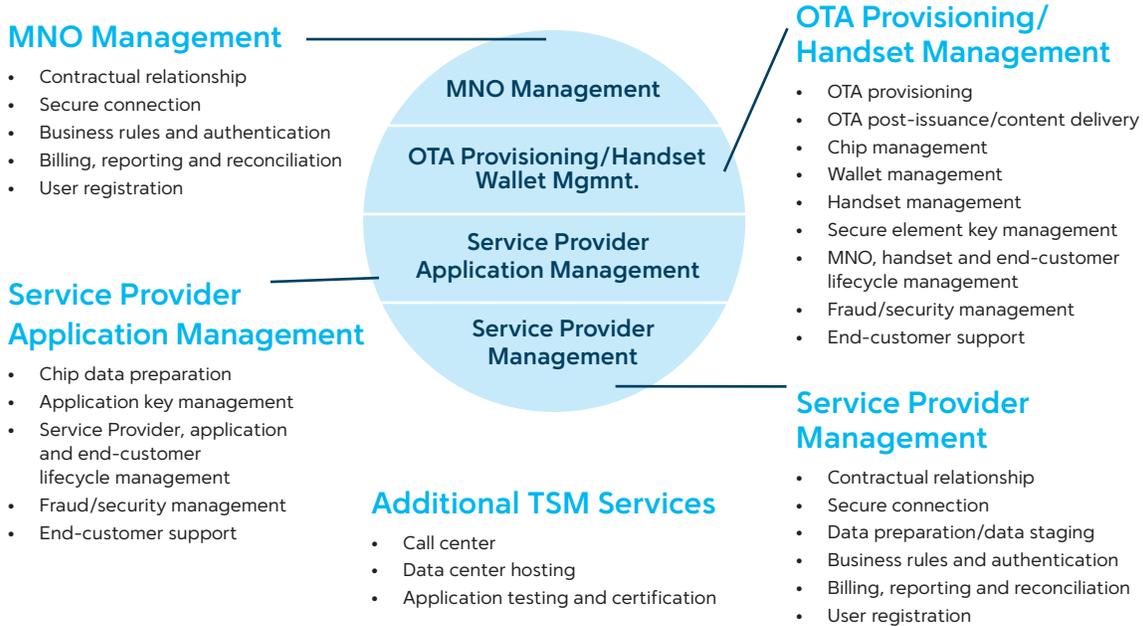
Finally, mobile subscribers must be properly authenticated before payment applications are provisioned to their mobile handsets. The TSM plays a key role in validating that the mobile subscriber is who he says he is,

that he is a valid customer of a given service provider, and that he has permission to receive a given payment application. All of this is information related to the TSM’s ability to manage “many-to-many” relationships across multiple service providers and multiple MNOs.

Let’s take a closer look at what an independent entity needs to be able to do to fulfill the TSM role.

## Key Capabilities of a TSM

The following illustration breaks down the essential tasks of the TSM into four broad areas of interdependent activities.



## Mobile Network Operator Management

TSMs will need to maintain contractual relationships with a critical mass of mobile network operators so that service providers’ NFC applications can be issued to a broad spectrum of end-customers.

For instance, if a large merchant wants to issue a loyalty application to its customers, or a major metropolitan transit authority wants to issue a ticketing application to its commuters, this makes sense only if the merchant or transit authority can reach most or all the potential consumers of these applications, regardless of what mobile network operators those consumers use. It’s not practical for every merchant, transit authority and bank to maintain its own contractual relationships with each mobile network operator. This would be a logical role for the TSM.

Part of the TSM-MNO relationship would include maintaining a link to the mobile network operator’s management systems for the purpose of providing a facility for customers of MNOs to register for commerce-related applications, providing for subscriber-related authentication on behalf of MNOs, and servicing individual accounts.

The TSM must also support administrative functions, including billing, reporting and reconciliation for TSM services provided to the MNO.

The TSM can also provide customer service on behalf of the mobile network operators for mobile subscribers with problems or questions related to NFC applications on mobile handsets.

## Service Provider Management

Service providers are those entities that offer consumer applications. These service providers might be merchants, banks, transit authorities, ticket agencies, health care providers or any of a number of other business entities.

The TSM will need to maintain contractual relationships with many thousands of service providers. This is not an insignificant task. There are over 8,000 banks in the United States alone, and thousands more businesses capable of offering consumer applications.

In addition to maintaining relationships with all these service providers, the TSM will also need to provide data staging for all the many different kinds of consumer applications, ensure the security of network connections through authentication management, and ensure conformity to business rules related to consumer account management.

The TSM must also support administrative functions, including billing, reporting and reconciliation for TSM services provided to the service provider.

Additionally, the TSM can provide customer service on behalf of service providers for account holders with problems concerning NFC commerce applications on mobile devices.

## Service Provider Application Management

There are other services that need to be performed related to service provider applications. For example, account and authentication data need to be configured for the specific secure element configurations on NFC mobile handsets. The function is referred to as chip data preparation. The TSM role also includes the complex task of securely managing service provider application security keys.

TSM systems maintain information about the life cycles of service providers, service provider end-customers and NFC applications used by service provider end-customers.

Finally, the TSM can play a role in helping service providers manage fraud and security related to NFC applications.

## OTA Provisioning and Handset Management

The TSM must be able to support the technical process for over-the-air (OTA) provisioning across different MNOs. This includes first-time provisioning of new applications to a secure element and post-issuance updates and content delivery.

The TSM also maintains information about handsets, chipsets and handset software (e.g., electronic wallet) required to ensure successful OTA provisioning to a variety of devices.

TSM systems maintain information about the life cycles of MNOs, MNO end-customers and the mobile handsets of MNO end-customers.

The TSM role can also include the complex task of securely managing secure element and security domain keys, and their relationships to NFC applications and NFC application keys.

All of the tasks outlined above that involve handling personal account information, security keys and user information will necessarily need to conform to industry security standards like PCI DSS.

So who among the many companies involved in commerce today has the resources and business model to fulfill the TSM role?

## Who Is Best Suited to Fulfill the TSM Role?

Clearly, the breadth of over-the-air provisioning services needed to support mobile commerce-enabled devices is far more involved than traditional credit and debit card provisioning. In fact, you might think there are few businesses equipped to take on this role. And yet as various players in the emerging mobile commerce ecosystem jockey to define their roles, almost everybody wants to be the TSM. Why?

The answer is quite simple. First of all, there will be fees associated with the TSM service. With over 3 billion phones in the world today, the fee revenue could be significant once legacy phones migrate to NFC-enabled phones capable of supporting multiple commerce accounts. Secondly, because no commerce can happen without applications in the phone, the TSM is in many ways the gateway to enable mobile commerce. NFC-based mobile commerce could soon represent significant consumer spending.

So, who are the TSMs in today's market? There's the rub. Although many companies today are interested in fulfilling this role, and a few might be able to do it, a true TSM does not exist today. The lack of a large-scale TSM solution is one of the key obstacles impeding market-wide acceptance of mobile commerce.

One reason there's no clear TSM solution is that many companies think they can provide this service, but in reality most companies that aspire to the TSM role are not yet capable of supporting all of the functions involved. Consequently, the industry has not yet worked out business models that will enable a large scale TSM to emerge. Let's take a closer look at some of the TSM aspirants.

### Mobile Network Operators

Because MNOs own the networks that provide access to mobile devices, they play an important role in the mobile commerce ecosystem. The TSM role would be a tremendous extension of the data services they already provide as well as (potentially) a significant source of revenue for them.

There is a catch, though: MNOs don't currently have the infrastructure for handling the vast amounts of application data and cryptographic data, nor do they have data centers that comply with banking-grade standards. Furthermore, they would need to establish many thousands of relationships with all the financial institutions that hold personal accounts, with payment card companies, processors, regulators and other entities—relationships they currently do not have. MNOs can, of course, develop the necessary infrastructure and business relationships, but they would need to carefully consider the cost and effort required.

Even more important, an MNO-centric TSM would create an inherent limitation on the size of the mobile commerce opportunity. Service providers desire to have coverage across their entire account-holder base, no matter which mobile network operator their customers use. A single mobile network operator, acting as a TSM, could not guarantee full account-holder coverage to any service provider.

### Card Associations

Card associations believe they are excellent candidates to fulfill the TSM role, and it makes sense from their perspective. The TSM role would make it much easier for the card associations to support their member financial institutions in the issuance of new payment applications and the expansion of the number of accounts they have. In addition, they already have an infrastructure in place for supporting their card accounts.

But there are concerns with this approach, as well. Card associations lack access to a complete set of banking data, and they might not be able or willing to reach agreements to share data among competing entities. This situation would likely force consumers to choose, for example, a mobile phone that is compatible with either Visa or MasterCard—but not one that works with both. No card association would likely give favorable treatment to

merchant programs such as prepaid accounts that completely bypass the traditional card instruments and card association networks, and yet such accounts are likely to be very popular with consumers and merchants alike, and could be a boon to mobile commerce.

## Financial Institutions

The TSM role is potentially attractive for financial institutions such as banks. By adding TSM-like services, a financial institution could position itself to control an end-to-end solution that serves its own customers with a convenient, new mobile offering. As an example, a major U.S.-based financial institution recently offered a bank-branded mobile phone with NFC-based mobile payment capabilities. But this bank-branded phone works only with the bank's own accounts. If a financial institution were to service accounts from its competitors, it would likely charge a fee for that service in order to steer consumers toward its own accounts.

With thousands of independent banks all competing for customers, it would be difficult to build the partnerships and alliances necessary to adequately serve multiple accounts from multiple banks across multiple carrier networks on a large enough scale to be effective. The market would fragment into mobile devices with limited purchasing capabilities, and this scenario would limit consumer acceptance of NFC phones as a replacement for the traditional wallet.

## Mobile Commerce Technology Solution Providers

As interest in mobile commerce has accelerated in recent years, many new companies have emerged that provide technical solutions required to enable mobile commerce. These companies are very important, because they have helped push the envelope on innovation and have proven the mobile commerce is technically feasible. These companies have helped make the general public, as well as other commercial stakeholders, aware of the possibilities of mobile commerce.

What these companies generally lack, and what impedes them from building full-service TSM businesses, are extensive relationships with service providers (e.g., financial institutions), MNOs or both. The business development activity required to build two-sided relationships to enable mobile commerce at scale can be more formidable and time-consuming than the development of technical solutions. In addition, as described above, a TSM must provide many supporting business services beyond just technical solutions. For sure, the technical innovators will play an important role in enabling mobile commerce, but might not be positioned well as stand-alone, full-service TSMs.

## Payment Transaction Processors

Third-party transaction processors, who currently perform most of the credit, debit and prepaid card provisioning, might be best suited to fulfill the TSM role. These companies now serve as multiple-account payment processors and card provisioners. In addition, they:

- Already have extensive relationships with banks, merchants, card associations and consumer-favored stored-value account service providers
- Have an enormous infrastructure for securely handling customer, financial and transactional data
- Are agnostic about the payment instruments they service—so they come closest to being able to offer a “free trade zone” in the mobile commerce economy

But they, too, need to forge new relationships, especially with mobile network operators, and expand relationships with banks if they are to fully service consumer account management.

## The Temptations and Perils of Segmented TSM Solutions

Many of the big, market-influencing players in mobile commerce are being tempted to take proprietary approaches to the TSM role so that they can preserve, monopolize and incrementally grow their existing market shares. At this early stage of NFC-enabled business, they also see this as a strategy for building customer loyalty by offering an exciting, new service.

However, this strategy will not be successful for long. Although it could attract customers initially, ultimately customers will discard devices with limited buying power in exchange for devices that offer them more universal purchasing and account management offerings. More important for the near-term adoption of mobile commerce, this approach restricts the utility of a mobile phones for commerce, and therefore reduces its value as a vehicle for target marketing. The overall effect will be to constrict the growth of mobile commerce.

In reality, the greatest opportunity lies in a neutral TSM entity, offering nonproprietary approaches. This is because a neutral TSM opens the entire mobile commerce economy to everyone and affords each of them the greatest opportunity to grow their positions through expanded service offerings. By enabling a single NFC-enabled device to contain a broad set of applications from multiple service providers, the neutral TSM can help not only increase the purchasing power of a mobile device, but also make the devices a much richer channel for target marketing and advertising. This will increase the value of the mobile commerce for all the participants—mobile network providers, merchants, financial institutions, advertisers or service providers in general and consumers.

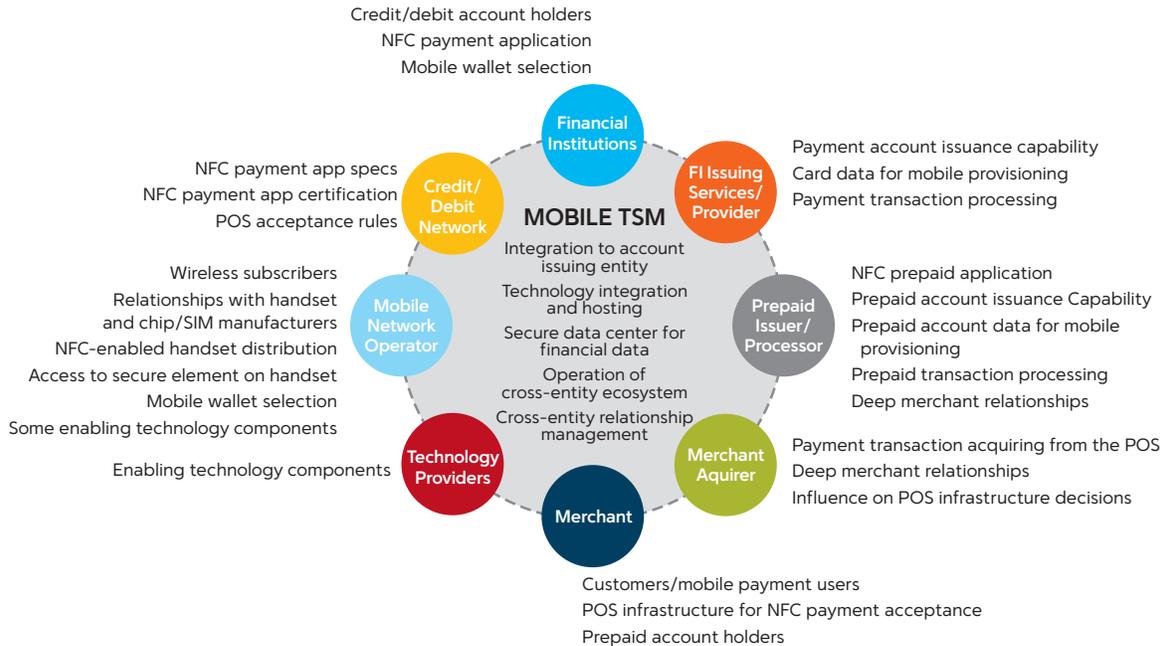
Think about it this way:

- If you are a bank and you want to broaden your customer base, you can promote your services to a much larger universe of potential customers, regardless of their location or mobile network operator, with the assurance that you can service all their accounts through an independent TSM
- If you are a mobile network operator, you want to be able to offer your customers as many NFC applications as you can because each one could be a source of revenue. You can do this through a TSM without maintaining a large amount of individual service provider relationships. This means you can increase revenue per user with far less cost and effort
- If you are a merchant, an independent TSM makes it much easier for you to offer prepaid accounts, loyalty accounts and special incentive accounts, regardless of the customer's location or mobile network operator

The surest way to a robust mobile commerce ecosystem is to maximize the commerce utility of each mobile device, and the best way to do that is through an independent, neutral TSM.

## Collaboration Is the Key to an Independent TSM

As illustrated in the diagram below, the TSM fills a critical role in the mobile commerce ecosystem, but is only one of a number of entities required to make mobile commerce happen at scale.



Certainly, no single organization has control over all of the assets and functions required to create an end-to-end mobile commerce ecosystem. But some entities are better positioned than others because they already fill more than one of the critical roles in the mobile commerce ecosystem. First Data, for example, already has a debit network, a financial institution issuing/processing business, a merchant-acquiring business and a prepaid issuing/processing business. By adding mobile TSM capabilities, a company like First Data could help drive the growth of mobile commerce. But partnership across the ecosystem is still important. The independent TSM will be essential for pulling together the right set of ecosystem participants and ensuring these participants operate together seamlessly. This step will go a long way toward maximizing the commercial potential of mobile commerce, as it would minimize the temptation of major players to fragment the market as they pursue their own special interests. This type of partner-driven TSM solution would result in a critical mass of consumer, service provider and merchant activity that would draw other participants into the fold.

In the early stages of mobile commerce, we are likely to see proprietary solutions with limited commerce potential. Over time, though, we will see the emergence of one or more large-scale, market-agnostic TSMs capable of supporting robust and diverse mobile commerce. The real challenge going forward, then, will be establishing business relationships to enable TSM solutions that maximize the buying and marketing power of each consumer’s phone.

For more information, check out the full mobile commerce white paper series at [firstdata.com](http://firstdata.com):

- The Risks and Opportunities in a Mobile Commerce Economy
- Mobile Payment: The Linchpin of the Mobile Commerce Economy
- Going Direct with Mobile Marketing
- Mobile Account Management: The Mobile Commerce Enabler

### The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

### About The Author

**Christopher Cox** is responsible for the development of First Data's Mobile Account Services product solutions. Chris and his team design, build and launch new products that enable First Data's financial institution and merchant clients create unique value for their customers by extending existing accounts and account-related functions to the mobile handset. Prior to his role on the mobile team, Chris was part of First Data's merchant product organization, helping to develop product strategy and assess new market opportunities.

Before joining First Data, Chris was a principal consultant with Diamond Management & Technology Consultants. At Diamond, Chris worked with Global

2000 companies to develop and execute technology-related business strategies. His project work was primarily focused on clients in the financial services and payments industries. Before Diamond, Chris was a staff consultant for CSC Consulting, where he provided technical and functional leadership on large-scale systems implementation projects.

Chris earned a masters in business administration from Duke University and a bachelor of science in mathematics from Miami University in Ohio.

**For more information, contact your  
First Data Sales Representative  
or visit [firstdata.com](http://firstdata.com).**