

E-Payments Primer

Third Edition

Prepared by the NECCC E-Payments Work Group



NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

Copyright © 2005 by National Electronic Commerce Coordinating Council

NECCC
2401 Regency Road
Suite 302
Lexington, KY 40503
(859) 276-1147
www.ec3.org

Made in the United States of America.



NECCC is a consortium of national organizations and public and private sector leaders
identifying best practices for strategic change within government.

Alliance partners are:

National Association of State Auditors, Comptrollers and Treasurers
National Association of Secretaries of State
National Institute of Governmental Purchasing

NECCC also works in partnership with these affiliate organizations:

Association of Government Accountants
Information Technology Association of America
National Automated Clearing House Association
National Association of Government Archives and Records Administrators
National Association of State Treasurers

Table of Contents

Introduction.....	1
Overarching/Crosscutting Issues.....	3
Customer Service in an E-Payment World.....	3
Authentication: Are You the Weakest Link?.....	4
Security.....	5
Privacy.....	8
Control Environment.....	9
Consumer Protection and Adoption.....	9
Tender/Payment/Receipt Types.....	12
Credit Cards.....	12
Debit Cards: PIN-Based and Signature-Based.....	15
Automated Clearing House (ACH).....	19
Stored Value Cards.....	21
Digital Cash.....	24
E-Wallets.....	26
Channels.....	29
Point-of-Sale.....	29
Telephone.....	29
Pay by Internet.....	30
Pay by Kiosks.....	31
Mobile: Cell Phones, Wireless, Radio Frequency Identification Devices (RFID) and Near Field Communication (NFC).....	33
Matrix of Payment Channels and Payment Types.....	35
Appendix A: Security Requirements for Payment Systems.....	37
Appendix B: Merchant Compliance Requirements.....	39
Appendix C: Parties Involved in Stored Value Card Management.....	40
Acknowledgements.....	42

Introduction

The purpose of this paper is to describe the current environment for electronic payments (e-payments) for the receipt of revenue for public sector organizations.¹ It is our intent that this information can help educate the various stakeholders on the issues, considerations, advantages and disadvantages of electronic alternatives to traditional methods.

According to statistics published by NACHA - the National Automated Clearing House Association, over the past 20 years the number of payment transactions in the United States has grown from approximately 40 billion (96% check, 4% electronic) to 95 billion (49% check, 51% electronic). As a general proposition this evolution from traditional methods to electronic alternatives has been mirrored in the public sector. However, as indicated in the statistics, there is still plenty of room for continued movement away from paper and towards alternatives.

NECCC has prioritized the area of e-payments in its work groups and research papers. In 1999, NECCC published an *E-Payments Primer*, which provided an overview of the electronic payment landscape. In 2002 it published an updated version of the *E-Payments Primer*, with particular emphasis on the issues, considerations, barriers, and benefits for public sector applications. In 2004, NECCC conducted a recognition program for public sector projects that exemplified best practices in e-payments. As a result of that work several significant projects and lessons learned were documented. Four projects were highlighted through the Excellence in E-Payments awards. In 2005, NECCC is continuing its examination and research in the area of e-payments.

The particular focus and topic for this paper is the application of e-payments as the method for the receipt of revenues to government, including various forms of taxes, such as personal income, corporate income, sales and excise (e.g., fuels, alcohol, and cigarettes and non-tax revenues such as fees, fines, licenses, sales, rents, assessments, reimbursements, grants, and gifts). It is typical for governments to include the receipt/revenue accounting functions as components of the respective business system, for example tax receipts associated with the tax administration system or drivers license fees related to the motor vehicle license/registration system. This paper is intended to focus only on the receipt/revenue accounting functions (not the complete business systems).

Regarding the revenue payer groups, the scope includes both companies and individuals. A particular focus is on revenue payers who are not in a routine and recurring relationship with the government (i.e., usually individuals).

Governments in a traditional approach receive revenue in the form of a physical check, either through the mail or over the counter. Upon receipt of the payment a manual workflow is employed until the check is deposited and the accounting data is entered into a computer system.

¹ For information on electronic disbursements, one source can be found at <http://ebt.nacha.org/docs/E-DOWWhitePaper-111403.pdf>

This primer will cover some basic aspects of e-payments. In the “Overarching/Crosscutting Issues” section (page 3), issues that are important to a successful e-payment program, regardless of payment instrument or channel, are introduced. The issues include a discussion of how customer service changes in a virtual world, how privacy, authentication and security issues must be addressed, and a general discussion of protections afforded to citizens who will use e-payment programs. In the “Tender/Payment/Receipt Types” section (page 12), various e-payment types are described according to the transaction flow, costs and benefits to government and risks. The “Channels” section (page 29), describes various established and emerging channels for e-payments. The final section, “Matrix of Payment Channels and Payment Types” (page 35), presents a matrix describing which payment types are appropriate in the various channels. After the appendices, a short glossary of terms is provided.

Overarching/Crosscutting Issues

Although payment types and payment channels for e-payments may vary, there are certain universal considerations that must be addressed in every case.

Customer Service in an E-Payment World

One of the most important elements of a successful e-payments project is customer service. This issue should be incorporated into an agency's change-management plan as part of an e-payment project. In 2004, NECCC conducted an awards program for innovative projects in the world of e-payments. Several customer relationship management themes permeated the submissions.

- Government customer service operations are typically not prepared to provide personalized service on a 24/7 basis, which is exactly what the average consumer expects based on his experience in the commercial world.
- For most agencies, citizens who are accustomed to face-to-face transactions expect personalized customer service. When new payment methods eliminate direct contact with employees, payers can't ask questions and resolve issues with a real person. This can cause frustration and negative feelings about new payment methods.
- Many successful projects noted that e-payments do not represent a change from one payment channel to a new payment channel, but rather the addition of one or more new payments channels to the traditional channels. It is important to decide how this new channel will be integrated with the existing CRM process.
- Finally we heard that customer satisfaction was tied heavily to the ease of the user interface. Projects with high levels of satisfaction involved customers as well as other stakeholders early in the project. Some held user focus groups to help design the customer interface; and others used pilot implementations to assess customer satisfaction. If the user interface is not efficient and pleasant to the customer, adoption will be significantly slowed.

Some questions for customer service employees will not be familiar because they deal with the new payment vehicles. For example, for credit card payments:

- How do I know that my credit card number is safe?
- How do I get a refund?
- How do I know I didn't get charged twice?

ACH payments (direct deposit) present a different set of inquiries:

- How do I know the money has been transferred?
- How do I know what the payment was for?
- What do I do if the bank says it didn't receive payment?
- How do I change my account number?

In your electronic-payments approach, you should decide if a centralized group will manage these citizen inquiries or if they will be referred to department/agency persons. It is important to note that no matter how you establish your customer relationship, existing staff will play a role. Employees well-trained on the new business processes will feel empowered and provide a positive citizen experience. Employees feeling suddenly overwhelmed and confused by new processes will convey those feelings to both internal and external customers.

Whether CRM is centralized or decentralized, the hand offs between organizations within the government must appear seamless to the customer.

Authentication: Are You the Weakest Link?

Electronic payment systems provide citizens with great freedom to pay for taxes, licenses, fees, fines and purchases at unconventional locations and at any time of the day, any day of the year. However, this increased flexibility comes with increased responsibility to ensure the security of the systems that underlie the transaction. These days, e-payment security is a hot topic. Major newspapers regularly include articles on new e-payment fraud, security threats and examples of electronic thefts. Chief information officers everywhere are directing their internal teams to implement multiple layers of security to protect vital financial information assets as well as other corporate information.

When payments are made outside of government centers where face-to-face transaction assure some proof of identity, how safe is that license renewal launched from the home office or a small business wireless network? E-payments are only as strong as their weakest link, and one of those links is knowing who is on the other side of the transaction – there are three criteria that will properly identify a legitimate participant. They are (1) *authentication*, (2) *authorization*, and (3) *access control*.

Authentication is basically a proof that someone or something is who he, she, or it claims to be. This normally involves a username and a password, but can include any other method of demonstrating identity, such as a “shared secret,” smart card, fingerprint, voice recognition, digital signature or even a retina scan. Authentication is equivalent to showing your drivers license at the ticket counter at the airport.

Authorization is finding out if the person or entity, once authenticated, is permitted to perform the requested transaction. This is usually determined by finding out if that person or entity is a part of a particular group, if that entity has necessary admission, or has a particular level of security clearance. Authorization is equivalent to checking the ticket when you go through airport security.

Access control is a way of talking about controlling access to a Web resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day or even the browser which the visitor is using. Access control is analogous to showing your ticket at the gate in order to get on the airplane.

For additional information, see http://www.ec3.org/Downloads/2004/identity_management.pdf.

Security

On a typical day at the end of 2004, approximately 70 million American adults logged onto the Internet to access e-mail, get news, access government information, check out health and medical information, participate in auctions, book travel reservations, research their genealogy, gamble, seek out romantic partners, and engage in countless other activities.²

As computers become more affordable, technology expands to new delivery channels like cell phones and PDAs, and high-speed broadband connections become ubiquitous, Americans expect to conduct their government business online.

According to the latest online retail sales data from the U.S. Commerce Department's quarterly survey, the estimate of e-commerce sales for the first quarter of 2005 was \$19.8 billion, an increase of 23.8 percent from the first quarter of 2004.³

As e-commerce grows, so do citizen expectations for online e-government services. Many reports indicate the convenience and usefulness of e-government services have improved citizens' perceptions of how government functions. Last year 29 million citizens researched or applied for benefits on government Web sites.⁴

Despite the fact that trends for e-commerce continue to climb, there are still millions of Internet users who refuse to conduct financial business, including purchases, online. A Visa USA Study released in 2004 reported that 83 percent of cardholders who have not shopped online say their reluctance is related to security fears that their credit card information is not safe.

² Pew Internet & American Life Project, January 2005, http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf 05/27/2005, Page 58.

³ United States Census Bureau, <http://www.census.gov/mrts/www/data/html/Q5Q1.html>.

⁴ Pew Internet & American Life Project, January 2005, http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf 05/27/2005, Page 66.

Reducing Security Fears

Ironically, paying by credit card is the safest way to transact business over the Web. Encryption and validation technologies have made most transactions very secure. Under U.S. law, the end-user's potential liability for unauthorized use of their credit card is limited to fifty dollars (\$50). Nevertheless, fears of online payment processing can be an obstacle for e-government acceptance and adoption. To minimize fear the government must reassure citizens that the transactions are safe.

Adhering to the Highest Levels of Security Standards

In order to accept credit card payments online, your organization must meet the Payment Card Industry's (PCI) Data Security Standards (DSS).⁵ The PCI Standard grew out of programs initiated by Visa and MasterCard. This consortium of credit card companies banded together to define a common industry standard for protecting cardholder account information across all card brands. Visa, MasterCard, Discover Card, American Express, Diners Club and JCB currently endorse this standard.

The purpose of the PCI Data Security Standard is to ensure that confidential cardholder information is protected from unauthorized access. The security requirements apply to "all system components, which are defined as any network component, server, or application included in, or connected to, the cardholder data environment."⁶

Because DSS requirements are far-reaching, following these mandates will ensure that your organization is conforming to an industry accepted and defined, quality security standard and provides citizens with faith that their government is committed to protecting citizen's privacy.

PCI Data Security Standard Requirements define 12 major requirements. Each requirement has several sub-requirements. See Appendix A (page 37) for details.

Who Must Comply and How?

All merchants (state or local agencies are considered merchants when they receive payments by credit card) that store, process or transmit cardholder data are expected to comply with the DSS requirements. However, compliance requirements depend on the number of transactions processed annually. See appendix B (page 39) for details.

⁵ Payment Card Industry Security Standards, Version 1.0, December 2004
http://usa.visa.com/business/accepting Visa/ops_risk_management/cisp.html.

⁶ Payment Card Industry Security Standards, Version 1.0, December 2004.

Merchants using third party providers or hosting companies are still responsible for compliance.

*"If there are service providers handling cardholder data on an entity's [Merchant's] behalf, the entity must ensure that contracts with these service providers specifically include [PCI DSS] compliance as a condition of business."*⁷

Consequences of Non Compliance

As with most regulatory requirements, PCI Data Security invokes penalties and fines for non-compliance. Merchants that suffer a security breach will also face penalties that vary by card brand.

Fines from card associations like Visa typically start at \$50,000 plus \$20 per card number compromised. Therefore, if 5,000 card numbers were compromised, a normal fine would start at around \$150,000. However, if the merchant is "compliant," meaning they can provide evidence that they are adhering to the requirements defined by their merchant level, the fine is typically waived.

Clearly Post Security Policies and Practices on Your Web Site

After your e-payment, infrastructure and processes are secure, it is also important to educate and inform your customers about the security and payment advantages you do provide. Post the certifications and security message clearly, so citizens do not have to search for them. Address the online payment process anxiety before it even begins.

For more information on Data Security Standards visit any of the following Web sites:

- Visa's Cardholder Information Security Program (CISP)
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
- MasterCard's Site Data Protection Program (SDP)
<https://sdp.mastercardintl.com/>

⁷ FAQ.pdf as provided by Visa for the PCI DSS

Privacy

"Imagine an industry with access to an unlimited supply of a highly valuable commodity, one that takes up little space, sells for billions of dollars and, best of all, is free."

"Sound like a deal you want in on? You are in. You're the commodity. We all are."

"Recent security breaches at data companies such as ChoicePoint and LexisNexis that allowed criminals to access the personal information of hundreds of thousands of consumers have highlighted not only the issue of criminal identity theft, but a sobering reality of the digital age. We don't own our identities. Data companies do."

These paragraphs from the May 28, 2005 issue of the *Miami Herald* dramatically convey the risks of doing business online. Specific laws will dictate whether or not data is available to the general public. But business practices will dictate whether or not the government is a deserving steward of the people's information. Remember, once electronic data is in the public domain, it will assume a life of its own as cyber data brokers replicate, store and share data *ad infinitum*.

Probably the most frightening result of poorly secured data is identity theft. According to www.white-collar-crime.com, identity theft is "the act of impersonating another, by means of using the person's information, such as birth date, Social Security number, address, name, and bank account information." Usually, the impersonation is for the purpose of assuming another's credit history in order to get credit for which the identity theft victim is then responsible. Identity theft is on the rise and is costing the U.S. millions in fraudulent credit. Serious adverse publicity is connected with companies and governments who were trusted with data and failed to protect it.

There are some basic principles that contribute to effective stewardship.

Don't collect data you don't need, especially social security numbers. Collecting information that is not required for the transaction creates an opportunity for that data to be stolen and misused. If there is no compelling reason to collect an item of information about the citizen, don't collect it.

Don't save data you don't need after the transaction is complete. Although it is convenient to keep credit card information for the citizen's next visit to a Web site, government sites probably don't have consistent frequent visitors. Every item of data that stored within reach of a cyber thief is an opportunity for identity theft.

Never display Social Security numbers. Social Security numbers are the key to citizens' credit records. An SSN is the closest thing in the U.S. to a federal government identity card. Treat it accordingly.

If personal information is ever released without authority, inform affected parties immediately about the breach. Several states have already passed laws that require notification of persons whose personal privacy has been compromised. Don't wait until your state passes a law—preemptively notify!

Perform background checks before hiring employees. Many cyber security breaches are made from within. A background check may detect a potential bad actor, or scare them off before you have to exercise the check.

If a payment system cannot afford the industry's best cyber security, then don't build it. The stakes are too high. If you fail to adequately protect the people's data, the damage done can outweigh all the benefits of convenience and speed.

Control Environment

E-payment projects frequently cite control and reconciliation between systems as a critical, yet often overlooked, step that can make or break an e-payment project. When governments move from paper-based to electronic business processes, the underlying principles of controls, risk assessment and risk mitigation apply. A well designed e-payment system can provide better controls and improved transaction visibility over conventional paper processes.

E-payment projects frequently involve adding Web technology (front ends) to legacy applications. Designing the reconciliation processes up front and automating them as much as possible is a significant success factor. During the 2004 NECCC E-Payment award program, designing the reconciliation process was repeatedly cited as a key success factor for those who built it into the original design and was equally cited as a lesson learned for those who failed to think through the process up front and struggled with controls and reconciliation during implementation.

Consumer Protection and Adoption

The electronic payment systems in place in the United States today are regulated by a number of government agencies and controlled by a variety of laws and regulations. Consumers are protected from a variety of misadventures when using these cards, thus affording a level of confidence when making payments electronically.

Citizens should understand the various governing regulations and play an active part in monitoring their financial accounts so that unauthorized transactions are identified, reported, and removed from their accounts.

Truth in Lending Act (TILA). Credit cards began as mostly local, proprietary merchant cards. While there was an effort to create widely held, general purpose credit cards, that effort did not pay off until Congress enacted federal billing dispute and unauthorized charge protections in the TILA. With these protections, credit cards instantly became more valuable than cash, especially for large transactions. Consumers who lost their credit cards or had them stolen would no longer be liable (at least beyond \$50) for unauthorized charges.

Consumers also gained from TILA the ability to dispute charges on their bills in a number of situations, including where a merchant did not deliver the goods. This gave consumers the freedom to deal with unknown merchants because they had recourse against their credit card issuer.

Electronic Fund Transfer Act (EFTA). As the name suggests, the EFTA focuses its protections on the transfer process rather than on the underlying transaction, and applies to non-credit card transactions. Two key protections relate to errors on the consumer's statement, such as the proper amount of the transfer, and limited consumer liability for unauthorized use. The EFTA is administered by a federal regulation referred to as Regulation E.

Uniform Commercial Code Articles 3, 4 and 4A. The starting point for determining rights, responsibilities and liabilities relating to forged, altered and other problem checks is the Uniform Commercial Code ("UCC"), Article 3, Negotiable Instruments, and Article 4, Bank Deposits and Collections. In these statutes you'll find important definitions, information relating to the customer's duty to examine his statement to discover and report alterations and forgeries, and much more.

The UCC has been adopted in all 50 states, although there are some variations in some of the provisions in a few states. A revised version of Articles 3 and 4 was adopted by nearly all of the states during the 1990s. Check with your staff attorney to determine what provisions in your state may differ from the uniform version.

Article 4A of the UCC deals with Funds Transfers and details how a bank can minimize its liability by having a commercially reasonable security procedure which has been agreed upon by the customer.

Office of the Comptroller of the Currency Banking Circular 235. Circular 235 was issued to alert national banks to the risks associated with large dollar payments systems, particularly within the international sector. This circular establishes the minimum standards for financial institutions subject to the jurisdiction of the Office of the Comptroller of the Currency regarding policies and documented procedures for electronic payments systems activities.

Regulation CC – Funds Availability. The Expedited Funds Availability Act was enacted by Congress in order to curb the unnecessary holding of funds by financial institutions. Although the regulation applies mainly to check transactions, there are provisions for funds deposited into an account by electronic payment (wire transfer or

Automated Clearing House credit payments). Under the regulation, funds must be made available no later than the business day following receipt of the funds.

Electronic innovations over the past decade provide consumers a variety of financial instruments and channels to make payments. Adoption of each depends on many factors such as lifestyle choices, life priorities, access to technology, convenience and consumers' personal experience with each.

Addressing consumers' concerns about electronic payments comes down to a few basics. First, the entity on the other side of the transaction (the government acting in the capacity of the merchant) must ensure that the tools they offer their customers are easy to use, cleanly designed so that they are intuitive, very reliable and constructed and operated in such a way that they offer secure and consistent service. Second, the merchant must proactively market the fact that they offer e-payment alternatives. Third, merchants must find ways to differentiate the e-payment options from other choices so that consumers want to use them. An excellent example is that most financial institutions and the major payment card companies have exceeded the regulatory requirements with regard to financial liability of unauthorized transactions. Despite the fact that the law stipulates that the consumer is liable for the first \$50 of unauthorized purchases, some banks and card companies have adjusted their policies and now actively promote zero liability for unauthorized transactions.

Despite consumer concerns about online transactions, the migration to e-payments continues to gain momentum in the United States, particularly among large corporations. In December, 2003 the Federal Reserve announced that e-payment transactions have for the first time exceeded check payments. In the United States, e-payment transactions totaled 44.5 billion in 2003, compared to 36.7 billion checks.

Clearly, the tide has turned. Similar research conducted by the Federal Reserve just four years earlier in 2000 showed check payments exceeding electronic transactions by a count of 41.9 billion to 30.6 billion. The Fed research reveals an average annual growth rate for electronic payments of 13.2 percent from 2000 to 2003, and an average annual decline in check payment volume of 4.3 percent.

For more information, consult "Electronic Bill Presentment and Payment Models" (online report) visit http://www.jpmorganchase.com/cm/ContentServer?cid=1107571610061&pagename=jpmorgan%2Fts%2FSTS_Content%2FGeneral&c=TS_Content, "E-Payment Migration Gaining Ground."

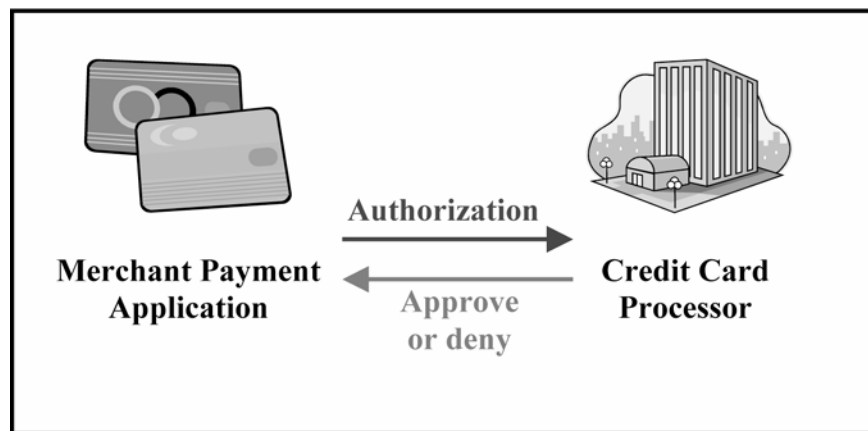
Tender /Payment /Receipt Types

In this section, we describe the current array of payment types.

Credit Cards

Credit cards work in an e-government application as they work in the physical world. Citizens enter credit card information into a Web application to pay for goods or services. Government's credit card application should invoke required data and business-rule edits to validate online data elements. Some of the edits could include user name, password, merchant ID, account number, expiration date, amount, and customer-billing data. Once the validity of required data has passed the credit card application edits, the authenticity of the cardholder's card ID and account number must be validated, and the transaction amount must be within the cardholder's credit limits. Processor-required elements could include merchant ID, account number, expiration date, amount, customer-billing data, card type, and Card Verification Value (CVV).

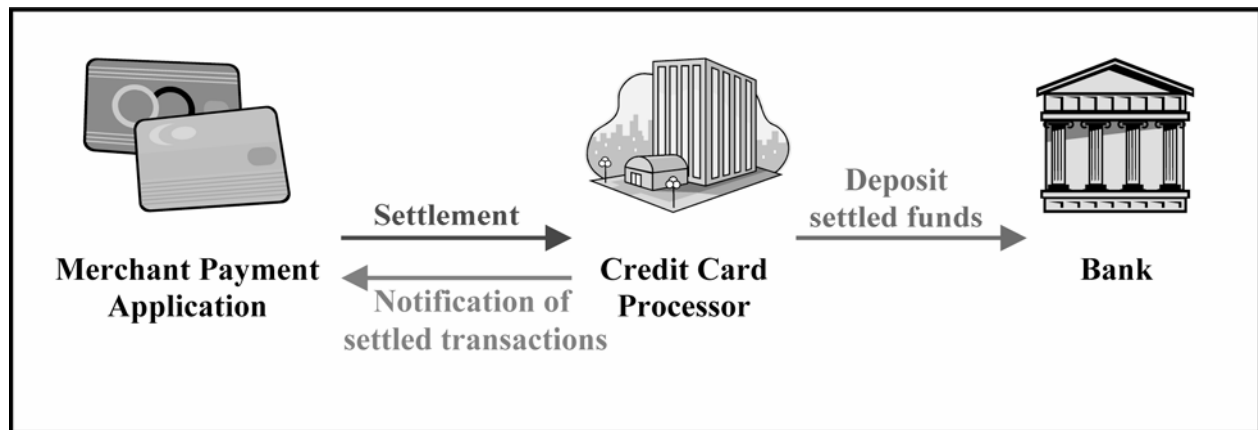
When all required edits are passed, the transaction is transmitted to the credit card processor and associated networks for authorization. The credit card-processing network returns an authorization approval, which indicates that the credit card is valid and the amount is within the cardholder's credit limit. A denial code will be returned when the credit card cannot be authenticated or credit limits have been exceeded. The opportunity to use another card or some other payment option might be offered.



Additional levels of card assurance can be obtained using Visa's Address Verification System (AVS) and the Credit Card Verification (CVV). These services work by validating the address of the customer or validating a code on the back of a credit card. They can help reduce fraud, chargebacks, and, possibly, merchant fees.

When an authorization approval is returned, the department's credit card application should acknowledge the approval of the transaction.

After authorization, the transaction must be captured when the goods or services have been provided, a process that is called "fulfillment." The credit card is billed when the goods or services are provided.



After a transaction has been authorized and captured, it is submitted to the processor for settlement in a batch with all authorized and captured transactions that occurred within a designated time period, usually a business day. This settlement-batch request usually occurs after normal business hours.

Following submission of the batch-settlement request, usually the following day, the processor will return a settlement acknowledgement to the government's credit card application, indicating that the batch has been accepted, will be settled, and a corresponding deposit will be made to the government's designated bank account. All transactions in the batch will be marked as settled. If the processor does not accept the settlement batch request, a failure code will be returned to the government along with its batch number and all associated transactions.

On a nightly basis, the government's application should create appropriate accounting transactions for credit card transactions that have been processed and approved.

Payment systems should also provide for voiding online transactions prior to settlement, issuing online credits, accepting reversal of approved transactions after settlement, and holding transactions from settlement pending fulfillment. For voids, the government application should have the functionality to mark a previously authorized/captured transaction as voided; voided transactions are not included in the settlement-batch request. For refunds, reversal of approved transactions must be initiated by the government, which must send data that

was obtained when the transaction was initiated, to the processor. In order for a government to use credit cards, it must establish a merchant account with the processor. The government provides the processor with the name, location, and routing transit number (RTN) of its destination bank, and the government's unique bank account number into which credit card proceeds will be deposited. In establishing these arrangements, the government will be required to comply with treasury or comptroller policies regarding the establishment and maintenance of cash accounts.

Within a specified timeframe, usually within 24 hours, the processor's acquiring bank will initiate a transfer for the amount of the settled batched transactions into the government's bank account. The Treasury will then "sweep" deposits from the department's account into the Treasury's bank account(s) on a regular basis and create a corresponding cash deposit transaction for each sweep.

Costs

The fees paid by government to the processor for credit card processing are determined by their contractual relationship and are based on a number of factors: total and average volume, total and average dollar amount, association fees, processor fees, card type, processing timeframe, etc. Payments to processors usually occur two ways: after processors send the government's gross proceeds from credit card transactions, they invoice government for their negotiated fees; or, if permitted, processors net their fees upfront and send the netted sales amount to departments.

Benefits to Government

- Reduced risk and costs associated with handling cash.
- Reduced risk and costs associated with handling checks.
- Reduced risk and costs associated with non-sufficient funds (NSF) checks and collection activities.
- Possible reductions in mail-handling delays and costs.
- Fewer errors and lost transactions.
- Faster fund deposit and availability at the bank, usually less than 24 hours.
- Improved turnaround time to customers.
- Increased opportunity for automation of accounting, banking and reconciliation processes.
- Opportunity for decreased costs though transactional volume available with centralized shared services.
- As customers shift to the Internet for services, some savings may be seen in reduced pressures on over-the-counter, mail, and phone customer-support services.
- Increased customer access (24x7 service availability).
- For automated systems, reduced transaction data-entry time.
- Impetus for various business re-engineering opportunities.

Challenges to Government

- Legislative issues:
 - o Credit card transactions may violate public-funds-handling laws.
 - o Justification of additional fees in legislative appropriation processes.
 - o Legislation fixes to protect financial data from public-records laws.
 - o Advertising and its associated revenue.
- New or increased costs associated with transaction charges and merchant fees.
- Handling fees through Generally Accepted Accounting Principles (GAAP).
- Increased costs associated with multiple decentralized applications and processes.
- One size does not fit all government agencies.
- Some initial costs to fund investment in technology and controls.
- Internet payments require new skill sets, business processes, and controls to mitigate exposures to new risks.
- Establishing and maintaining new, statewide security standards.
- Costs of integrating legacy mainframe systems to current Web-based technology.
- Anticipating Internet adoption rates for government goods and services.

Debit Cards: PIN-Based and Signature-Based

A debit card is a card which physically resembles a credit card, and like a credit card, is used as an alternative to cash when making purchases. Unlike a credit card, however, the funds are withdrawn directly from the purchaser's checking or savings accounts at a bank. While a credit card is a way to "pay later," a debit card is a way to "pay now." Debit cards are accepted at many locations, including grocery stores, retail stores, gasoline stations, and restaurants. Debit cards can be used anywhere merchants display the card's brand name or logo. Debit cards offer an alternative to carrying a checkbook or cash. Debit means "subtract." When a debit card is used, money is subtracted from the related bank account. Debit cards allow only the amount in the bank account to be spent and provide for quick transactions between merchants and personal bank accounts.

"Online" debit cards are usually enhanced ATM cards that work in the same manner as an ATM transaction, allowing for an immediate electronic transfer of money from a consumer's bank account to a merchant's bank account. To access an account at a store terminal, a PIN must be entered, just as in an ATM transaction, giving the system authorization to check an account to see if it contains enough money to cover the transaction.

"Offline" debit cards usually look like credit cards and their transactions resemble credit card transactions. These cards carry the same logotype as the major credit cards. The merchant's terminal reads the card, identifies it as a debit rather than a credit card, and creates a debit against the customer's bank account; however, instead of debiting the corresponding account immediately, it stores the debit for processing later. Most but not all offline

debit transactions are verified to see if adequate funds are available. Instead of using a PIN number to complete such transactions, the customer signs a receipt, just as with a credit card transaction.

When debit card transactions are initiated from a government or department Web application to pay for goods or services, they require a different approval process. Checks and edits for required data are applied, and an approved transaction is stored for transmission to the ACH.

Costs

As the focus of this document is electronic receipting, the issue of interchange fees needs to be discussed. Governments seeking efficiencies with electronic receipting often express concerns over the interchange fees associated with card-based payments. Fees paid by government “receipters” of card-based payments are most typically a percentage of the transaction amount, sometimes also including a small per transaction charge. A variety of factors determine the fee a banking institution charges (or negotiates with) clients. These factors include:

- 1) Credit Risk – This is the risk that the payee cannot or will not fund the payment of the transaction. Credit risk is low or non-existent with debit cards, particularly as opposed to credit cards. Most debit card transactions include online validation of funds, virtually eliminating the risk that funds will not be “good.”
- 2) Card Administration Costs – Banks incur administrative costs for card issuance, processing, statement production, etc. Most card administration functions are outsourced by banks, to third party service providers such as Total Systems or First Data Resources.
- 3) Fraud Risk – This is the risk that the transaction is being fraudulently conducted by the payer. A stolen card or stolen card number is the most common form of fraud. Where merchants do not exercise appropriate due diligence at the point of sale, banks may impose the responsibility for card fraud on merchants. With debit cards as opposed to credit cards, financial responsibility for fraud may more often be imposed on the card holder.
- 4) Cost of Funds – This is the time value of money between the time the transaction is consummated and funds are forwarded to the merchant, and the time the cardholder pays the bank. This issue is minimal for debit cards, and has less of an impact on banks where consumers carry an unpaid balance from month to month (interest begins accruing to the card holder when the transaction reaches the credit card network).

For purposes of discussion, the following table attempts to compare and contrast the cost components for debit and credit cards, and offers an estimated average interchange fee for each type of card:

<u>Cost Component</u>	<u>Debit Cards</u>	<u>Credit Cards</u>
1) Credit Risk	Substantially Lower	Substantially Higher
2) Card Administration	Somewhat Lower	Somewhat Higher
3) Fraud Risk	Lower (esp. PIN-based)	Higher
4) Cost of Funds	Lower	Higher
Total	<u>175 basis points</u>	<u>225 basis points</u>

The table does not include a specific estimate of the portion of interchange fee allocated to each cost component. The interchange fee is a subject of much discussion and debate in the merchant and banking community, and is most often uniquely negotiated between banks and merchants. What could be argued from a review of the above table is that many of the cost components associated with debit cards are lower, however estimated average interchange fees for debit cards are still substantial in amount.

An in-depth discussion of debit card fees is beyond the scope of this paper, and the above attempt to decompose the interchange fee undoubtedly raises more questions than it answers. But de-mystifying fees associated with e-payments is essential for greater adoption of electronic receipting by government. Merchants and banks with a shared and common understanding of these fees will make better business partners.

At this point in the evolution of debit cards and their associated fees, debates over the appropriateness of these fees have resulted in legal action. Legal action about debit card fees often addresses the broader issue of interchange fees as it affects both debit and credit card transactions. Readers interested in more should learn about the Wal-Mart class action suit against VISA and MasterCard that resulted in the temporary reduction in interchange rates for PIN-based debit cards.⁸

Benefits to Government

Many of the benefits debit cards offer government are the same as those offered by credit cards, namely:

- Improved cash flow.
- Reduced operating costs.
- Streamlined debit card acceptance procedures.
- Simplified payment and collection processes.
- Simplified record keeping.

⁸ <http://www.cardforum.com>; <http://www.sourcemediacom.com>;
http://www.kroger.com/press_tmp.asp?fileId=07152005&Category=speeches&SubCat=newsspeech

- Increased potential for consumer and citizen services including earlier receipts of payments due.
- Added convenience for citizens.
- Enhanced fraud protection.
- Better control and transparency in the use of resources.

Additionally debit cards may provide advantages to governments over credit cards:

- Obtaining a debit card is often easier than obtaining a credit card, creating more potential users.
- Returning goods or canceling services purchased with a debit card is treated as if the purchase were made with cash or check.

Challenges to Government

- *Using debit card PINs over the Internet.* In a financial network, PIN security is dictated by the network rules. Network rules cover a wide range of topics including transaction processing, card sponsorship, membership, security, adjustments, etc. These rules currently require Triple DES encryption and the use of a Hardware Secure Module (HSM) or a Tamper Resistant Module (TRM). ATM key pads and point-of-sale key pads are either HSM or TRM compliant. The keyboard of a desktop/laptop computer is not HSM or TRM secure.
- *PIN-less debit is supported by various networks (NYCE, STAR and PULSE, etc.).* This is a wrinkle that has been added to the current PIN DEBIT/Signature Debit products offered by the various credit card associations/companies. The product was originally developed specifically for utility companies. A recent PULSE newsletter indicates that PULSE has expanded its program to include government agency payments (tax, fees, fines and penalties), educational payments (tuition, room and board and alumni), insurance payments (property, casualty, health and life) as well as loan payments (real estate and motor vehicles). As the name implies, an Internet-originated PIN-less bill payment uses the consumer's ATM/debit card number that is entered at a PC, but does not require a PIN for authorization. It is unclear as to whether the other networks support this expanded list of options. There is some confusion with this product. A look in your wallet might find a MC/VISA debit card that was issued by your financial institution for your use at ATM's and POS locations. If you look on the reverse side of the card, you might also find a local area network logo (STAR, NYCE, PULSE, etc.). This card could be used in a PIN-less debit environment as well as the standard ATM and POS applications. Determining what companies participate in the PIN-less debit program will require some research. Another aspect for consideration is that PULSE advertises this product to its financial institutions as a money maker with an interchange fee of \$.35 per transaction. Certainly other participating networks have similar fee structures.

Risks to Government

PIN-less debit transactions do go through an online authorization process and have the same guarantees as the credit and signature debit (subject to unauthorized transaction claims). PIN-less debit transactions are purported to be approximately 50 percent lower in cost when compared with credit and signature debit.

Automated Clearing House (ACH)

The ACH Network is a processing and delivery system that provides for the distribution and settlement of electronic credits and debits among financial institutions. Through a nationwide telecommunications network, each ACH operator is able to communicate with other ACH operators to exchange entries quickly and efficiently, regardless of geographic distances involved. The ACH Network is governed by operating rules and guidelines, which are developed by the actual users of the system, and is administered through a series of agreements among financial institutions, customers, trading partners, and ACH operators.

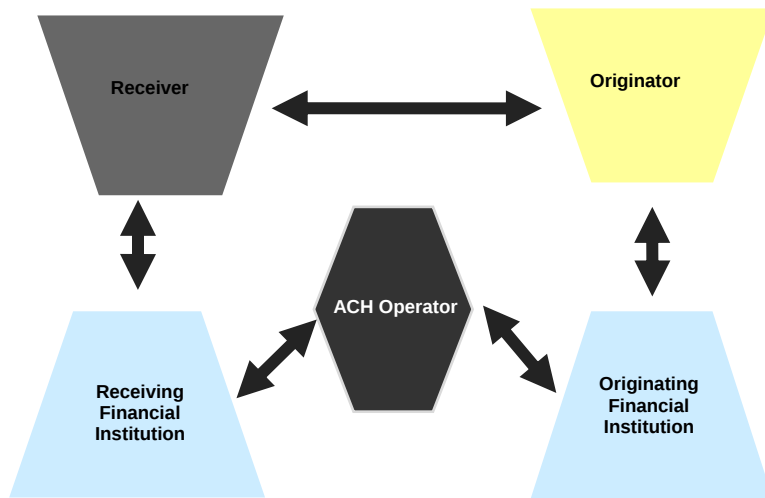
The ACH Network is a batch processing, store-and-forward system. Transactions received by the financial institution during the day are stored and processed later in a batch mode. Rather than sending each payment separately, ACH transactions are accumulated and sorted by destination for transmission during predetermined time periods.⁹

The parties that must participate in the process for ACH transactions include:

- *Originator* – An individual, corporation or other entity that initiates entries into the Automated Clearing House Network.
- *Originating Financial Institution (ODFI)* – A participating financial institution that initiates ACH entries at the request of and by agreement with its customers.
- *ACH Operator* – A Federal Reserve Bank or an entity that executes an annual agreement with the national association to comply with and perform clearing, delivery and settlement services for ACH entries.
- *Receiving Depository Financial Institution (RDFI)* – Any financial institution qualified to receive ACH entries that agrees to abide by the NACHA operating rules and guidelines.
- *Automated Clearing House (ACH) Network* – A funds transfer system, governed by the NACHA operating rules, that provides interbank clearing of electronic entries for participating financial institutions.

⁹ 2005 ACH Rules, The National Automated Clearing House Association
E-Payments

Transaction Flow



All parties to the ACH Network must have agreements with one or more of the other parties that bind the participants to the NACHA operating rules and guidelines as well as federal rules and regulations.

Cost to Government

ACH transaction pricing is negotiated between the originator and ODFI and encompasses all of the same types of services and fees that would accompany a transaction account. On an individual transaction basis, there are basic fees for origination and receipt that can vary from \$ 0.029 to \$ 0.10 depending upon volume and compensating balances. ACH entries are batch processed and have required settlement dates. There are no start-up costs and no special software requirements depending upon whether the governmental entity is capable of generating its own files and entries.

Benefits to Government

- ACH is electronic and by definition there is an overall reduction in paperwork associated with the entries. Direct deposit is the transaction which is most commonly associated with ACH. However, ACH transactions are both debit and credit.
- Settlement dates provide predictability of funds flow.
- Since this is a financial network, agreements clearly define the liabilities and responsibilities for ensuring the fiscal soundness of the transactions.
- *Electronic lockbox processes that employ check conversion accelerates the collection process and can be integrated with accounts receivable applications.*

- Regional ACH associations provide low-cost training and education services, associate membership programs and on-site audit reviews. Most ACH associations have help desks which can be accessed by both members and non-members. The national Web site is www.nacha.org. There is a map associated with this site which leads viewers to regional Web sites.
- ACH cost compares favorably with credit, check and debit.
- ACH check conversion programs have a wide range of third party processors who can integrate the ACH application with existing debit/credit point-of-sale software.

Challenges to Government

- Payment processing at the state level is generally handled on an individual department/agency basis. This decentralized approach leads to redundant procurement processing, proposal preparation and response evaluation. Once awarded, this decentralized process means software expenses are paid multiple times. The practice also precludes the government from negotiating the best price based on volume and aggregate risk. The challenge is to view payment processing on a statewide level to take advantage of volume pricing and discounts.
- Currently, ACH products have two distinct transaction classes. The business products class does not support check conversion, while a wide range of products for check conversion are available in the consumer class.
- ACH does not afford the citizen the same protections as are afforded credit card users.

Risks to Government

- Consumer ACH payments are subject to the Regulation E, right of rescission. The check conversion applications are subject to stop payment, insufficient funds and the added Reg. E return as unauthorized.
- ACH payments are batch processed versus online authorized which can lead to returns. Return items can be reprocessed.
- Return item risk can be mitigated by reversing the original transaction and an aggressive process of collection, utilizing various penalty options such as late fees, interest accruals and revocation.
- Since there is a different set of rules for business versus consumer, two processing streams must be developed to deal with two payment channels.

Stored Value Cards

Stored value cards are most commonly used as a disbursement method by governments, but in this primer we consider their use as a payment mechanism.

Governments generally accept these cards over open networks that utilize point-of-sale debit or credit networks, such as MasterCard, Visa, Cirrus, Plus, STAR and NYCE, etc. The point-of-sale may be a government office or a

kiosk in a public place. There are a variety of applications for prepaid cards, including gift cards, payroll cards, flexible spending account cards, government benefit cards (such as food stamps), insurance claim cards, employee reward cards, travel cards, remittance payment cards, and transportation cards.

It is important to understand the roles and responsibilities of several of the key stakeholders in the stored value card chain. Appendix C ([page 40]) contains a chart that briefly describes the parties involved in the ongoing management of any stored value card program.

There are many laws, regulations and industry practices that are designed to protect consumers who use stored value cards. Most of these are consistent with existing protections for any cardholder using a credit or debit card; however, there is increased scrutiny of stored value cards specifically.

Existing federal and state protections and network operating rules are available to debit cardholders who face fraud, error or disputes with merchants (government). This paper cannot adequately describe all of the regulatory or legislative initiatives that have surfaced recently pertaining to stored value cards, but most address the following general topics:

- *Definitions*
 - o Uniform distinctions and product definitions (i.e., gift vs. general purpose vs. government disbursement, etc.)
- *Fees and Disclosures*
 - o Highlighting benefits relative to fees
 - o Supporting full disclosure
- *Expiration Dates*
 - o Expiration of plastic vs. expiration of the funds
 - o Security issues
- *Abandoned Property*
 - o State vs. consumer vs. issuer
 - o Anonymous card
- *Payroll*
 - o Authorization of use
 - o Access to funds
 - o Fees

Notwithstanding the industry's efforts to make protections more uniform, the laws and regulations that apply to stored value cards remain complex and rapidly changing. FDIC insurance coverage may apply to individual cardholder "accounts" or apply only to the pooled or aggregated account held at the issuer financial institution.

Costs to Government

Stored value cards can be implemented in many different ways and cost considerations are unique to each kind of implementation. Since adoption of stored value cards is limited, it is unlikely that government will adopt this form of payment. If a government decides to implement stored value cards, costs should be researched and considered in that case.

Benefits to Government

The stored value card programs are primarily considered replacement products and are targeted at existing programs to reduce or eliminate paper checks or voucher programs. This replacement feature represents the most significant short-term opportunity and eliminates much of the need and cost associated with recipient adoption or enrollment. Listed below are the most compelling benefits in considering stored value cards:

- Reduces costs associated with check and voucher processing; savings can be redirected to other program improvements.
- Depending on program design, card acceptance can be either no-cost or low-cost to the government payment unit.
- Eliminates bad checks.
- Reduces fraud inherent in lost and stolen checks and vouchers.
- Enhances payment security through authentication at POS and kiosks.
- Provides service to unbanked citizens by giving them the opportunity to participate in mainstream financial services, other than check-cashing and other high-cost money services.

Challenges to Government

Since open network stored value products are relatively new to this market, the challenges faced by government focus primarily on adapting processes and systems to a new payment method. Here are some challenges that should be considered:

- Some programs may be designed to restrict usage of funds to specific merchandise or commodities which may require specialized transaction processing, reporting and monitoring (i.e., emergency disaster relief).
- Training is required for internal agency staff so that they are comfortable with the card usage, client service and error resolution.
- Card accounts can be “overdrawn” in certain specific situations.

Digital Cash

Digital cash is a tool that allows a person to purchase goods or services by transmitting a number (value) from one computer to another. The individual first sets up a digital account with a bank or other provider. Then, a limited sum is transferred from an existing bank account or credit card into the digital account. This may be in the form of anonymous or identified digital cash. When the person makes a purchase, the amount is transferred from his or her digital account to the account of the vendor.

Each digital cash number is issued by a bank and is unique, much like the serial numbers on paper currency.

Anonymous digital cash, like currency, cannot be traced through the economy and is reusable. It is not possible for the vendor to obtain information about the payer. This is a major distinction between credit card and digital cash systems.

Identified digital cash includes information about the person who originally withdrew the funds from the bank. This allows the bank to track the money as it travels through the economy.

As with currency, protective action must be taken to guard against duplicating or counterfeiting digital cash. Any successful digital cash system must be designed so that a piece of digital cash cannot be copied and both pieces spent, a process referred to as “double spending.”

A good digital cash system must provide users with security and privacy and requires cryptography with strong algorithms that are virtually unbreakable. Secure key management is also critical.

To use online digital cash, users must interact with a bank, via a modem or network, to carry out a transaction with a third party. The merchant contacts the bank's computer with every sale. The bank verifies that the digital cash number has not been previously used, approves the transaction for the vendor, and then updates its database to reflect use of the number.

Offline digital cash processing is more complex than online processing, due to the greater difficulty in protecting against counterfeiting and fraud. One way to protect against fraud is by using a smart card that keeps a record of all the numbers of digital cash transferred and subsequently spent. Another way is to design cryptography protocols in such a manner that fraudulent, or double, spenders are known by the time digital cash makes its way back to the bank.

Costs

It was difficult for the authors to find information about the costs associated with digital cash, but it was found that costs for processing digital cash are less expensive (in some cases, near zero) than credit cards, primarily due to the fact that transferring digital cash via the Internet is less expensive than through the conventional banking system.

Benefits

There are advantages to using digital cash as a payment mechanism:

- Reduced cash handling, check handling, or credit card processing.
- Faster value into the bank.
- Elimination of collection risk; checks and credit cards can reject or “bounce.”
- Reduced debt-collection efforts.
- Improved customer service.
- Reduced postage fees and postage-paid return envelopes.
- Timelier reporting.

Challenges

- *Fees*

If there are fees associated with the digital cash system, every government will have to determine who absorbs those fees. Consideration must be given to political as well as financial ramifications. For example, an individual purchasing a recreational permit may find it acceptable to pay a nominal charge for having the choice of a payment method. However, it may be more prudent for the government to accept the fee as a cost of doing business and as an incentive for prompt payment of mandatory payments such as income or property taxes.

- *Lack of Customer Experience*

Another common problem with digital cash is the lack of hands-on experience in dealing with it. Few people have actually used digital cash. Again, the lack of experience primarily ties to the fact that digital cash has not become a dominant player in the market. As more companies offer credit card payments via the Internet, there seems to be less interest in fully pursuing alternate avenues. From a governmental perspective, not only does the government have to figure out how to implement such a system, but it also needs to figure out how to make it completely accessible to end users. Digital cash purveyors may develop standards that would make digital cash transaction more uniform and thus more common.

Risks

One of the primary reasons for the lack of development in the digital cash/e-wallet arena is the lack of standards and protocols. With each new form of digital cash, there seems to be a slightly different set of standards and protocols. Keep in mind that in order to use digital cash, both the payer and the payee must be previously set up to use the specified form of digital cash. At this point, no one form of digital cash has become a dominant player in the industry. Therefore, there are different types of digital cash becoming localized in different geographic areas. If one standardized form of digital cash becomes dominant in the marketplace, usage of digital cash will become more commonplace.

E-Wallets

E-wallets allow consumers to register and enter personal and financial information once into a form and have the e-wallet auto-populate forms on a recurring basis

An e-wallet is a secure, virtual container that holds a consumer's personal data and presents that data to a merchant at the time of the purchase. An e-wallet must be secure because, as in the physical world, possession of personal data, especially financial data, by malicious persons could result in fraud. An e-wallet is a piece of software that emulates on the computer screen what shoppers do in a retail store when they want to make a payment choice. Containing and transmitting both payment and shipping information eliminates the annoyance of filling out multiple pages of order forms.

Basic E-Wallet Functions

- Management, tracking and exporting receipts and other purchase information.
- Enabling of bill-presentment solutions.
- Loyalty-program tracking.
- Facilitation of micro-payments.
- Creation of online allowances and other spending-control systems.
- Relationship mediators.
- Monitoring of user's online purchasing profile, assisting with pre- and post-purchase support, and acting as trusted agents and marketing filters.

Costs

Rates for e-wallets are similar to credit card and additional associated costs that result from a poor adoption rate. It was difficult for the authors to locate material about the costs of e-wallets.

Benefits

E-wallets, such as PayPal allow international payments to be issued to anyone with an e-mail address, free, anytime, for any reason. PayPal provides securities against fraud, such as FDIC pass through insurance, money back guarantees, user verification, privacy policies, etc. Utilizing e-wallets such as PayPal permits purchases in various currency exchanges at no additional costs. With online auction houses such as eBay (acquired by eBay in 2000), PayPal is a crucial aspect of conducting online transactions.

Some additional benefits:

- Constituents do not need to fill out multiple forms at each site, reducing the abandonment rate for online purchases.
- The rate of errors on order forms is reduced.
- Constituents are encouraged to shop online.
- Could establish a linkage between constituent e-wallet and an EBT card to set up the e-wallet account, providing additional value to a broader group of constituents.
- Analysis of purchasing patterns and targeted pricing allow the constituent to have appropriate information pushed to his or her wallet.
- Ease of government tracking of the use of EBT cards, when linked.

Challenges

- The thick client model requires constituents to download software to their personal computers and then to update the e-wallet when changes occur. Broad usage may not be practical.
- May be a significant financial investment for little real benefit to the constituents; most of the benefit is for government.
- In the calculation of return on investment, it is important to include costs to agencies that may be significant in terms of infrastructure and customer care to manage processes such as authentication and privacy. Instead of providing financial benefits, e-wallet eases the collection of demographic and buying histories.

Risks

The use of e-wallets will present some risks to government:

- Lack of standards and lack of universal merchant acceptance for e-wallets.
- Privacy and trust issues arise with e-wallet vendors taking and storing personal constituent information. Constituents may be reluctant to trust this information to relatively unknown e-wallet vendors or to government agencies.

Additional information is available from e-wallet providers' links (this is not an exhaustive list).

PayPal

San Jose, CA

Internet: <http://www.paypal.com>

Telephone: (402) 935-2050

Products: PayPal Accounts

Gator.com

2000 Bridge Parkway, Suite 100

Redwood City, CA 94065

Telephone: (650) 232-0303

Facsimile: (650) 232-0303

Internet: <http://www.gator.com>

Products: Gator Wallet

IBM

New Orchard Road

Armonk, NY 10504

Telephone: (914) 765-1900

Facsimile: (914) 765-4190

Internet: <http://www.ibm.com>

Products: IBM's Consumer Wallet

Microsoft

1 Microsoft Way

Redmond, WA 98052

Telephone: (425) 703-5529

Facsimile: (425) 936-4112

Internet: <http://www.PassPort.com>

Products: PassPort Wallet

Channels

In this section we will describe the current array of e-payment channels.

Point-of-Sale

Point-of-sale is software to operate a flexible and automated cash management system. In addition to integrating all the components of a point-of-sale system with a central computer terminal, point-of-sale software typically offers sophisticated organization capabilities. It provides for detailed financial reporting, enables inventory tracking in real-time, allows capture of all customer information for improved service, offers integrated credit card processing, which means you don't have to re-key accounting or credit card information, and permits flexible configuration with checks to prevent your staff from making errors.

Point-of-sale systems allow the public to pay for goods and services with debit cards and credit cards, checks and cash over the counter at walk in service centers. The program provides the public with a cost-effective convenient way to pay for government goods and services and allows for quick and efficient updates to citizens payment records.

The point of sale is a location where credit card transactions are performed with the cardholder present. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.

Telephone

Interactive Voice Response (IVR) is a telephony technology in which someone uses a touch-tone telephone to interact with a database to acquire information from or enter data into the database. IVR technology does not require human interaction over the telephone as the user's interaction with the database is predetermined by what the IVR system will allow the user access to. For example, governments use IVR systems so that their customers can receive up-to-date account information instantly and easily without having to speak directly to a person. IVR technology is also used to gather information, as in the case of telephone surveys in which the user is prompted to answer questions by pushing the numbers on a touch-tone telephone.

IVR or pay-by-phone systems eliminate inconvenience and costs associated with postage and check-writing. Studies have shown that electronic bill payment reduces these costs by 60 percent by eliminating the cost of stamps and paper checks and by reducing consumers' exposure to late fees and bounced checks.

The costs associated with a pay-by-phone system will depend on the hardware and software needed to launch a system into production. There are some vendors who are willing to launch a pay-by-phone system with no startup costs by charging the payer a convenience fee to recoup development costs.

Deploying a pay-by-phone system allows government to collect payments without having to employ additional staff. It allows users to pay for transactions 24/7, increasing collection opportunities.

One of the main challenges of a pay by phone system is to develop verbiage scripts that ensure ease of use for payers.

Customer information is collected and there is always the risk of fraud attacks through virtual channels. Fraud prevention measures should be taken to reduce the risk of fraud.

Pay by Internet

An Internet payments application allows governments to accept credit card payments and electronic funds by Web. With the ability to receive payments for government services online, municipalities can move beyond providing information to conducting transactions. This is a key component of government electronic service delivery.

Using credit cards and electronic checks to purchase government services or pay taxes over the Internet is relatively new for many public sector jurisdictions.

An Internet payment application reduces the costs associated with traditional, and inefficient paper-based methods of payment and allows citizens to access goods and services when and where it is convenient for them. This will significantly improve access to government services.

There are many costs associated with developing and maintaining an Internet payment site. These costs include hardware, software, licenses and maintenance costs. Depending on the level of functionality built into the application, these costs will vary.

Efficiency and Effectiveness of E-Payments

The electronic filing and payment of taxes and fees have been proven to be both efficient and effective. Fewer errors lead to faster processing time for the government entity. In addition to providing faster service, credit or debit card payments made by consumers are subject to real-time authorization and verification. Time waiting for the check to clear is eliminated. Simply put, the government entity receives payments faster.

- Delivery of services 24 hours/7 days a week to the public over the Internet.
- A reliable and secure way to access and pay for government services.
- Automation of government business processes.
- An Internet payment program will enable government to shift from traditional over-the-counter services to online services where the public can pay for goods and services over the Internet, and where payments can now be accepted for many informational programs that are already online.

An e-payment project can face several obstacles within a bureaucracy, at the political level or with outside entities. Some issues that may exist within a bureaucracy:

- Who takes ownership, responsibility and the lead in a project?
- Turf wars that can lead to hostility.
- Keeping enthusiasm for the project.
- Leadership continuity issues.
- Overcoming implementation difficulties regarding standard systems, legacy systems, budgets.
- Union, middle management opposition.

At the political level:

- Inadequate funding or allocation of resources.
- Legislative or regulatory constraints.
- Political opposition.

Outside Entities:

- Gaining public trust.
- Reaching your audience (digital divide).
- Handling opposition from competition.

Citizens' information must be kept secure and confidential. Hackers present a risk if this private information is revealed.

Pay by Kiosks

Today's public sector organizations are using kiosks to give citizens better service and support, and ultimately, a lower-cost government. These organizations are implementing self-service kiosks to provide access to an array of services from property tax payments, vehicle registration, permitting and licensing. The use of kiosks has also been driven by the public's demand for increased hours of business and shorter wait times.

A kiosk consists of a touch-monitor, a computer, and perhaps a printer and credit card reader—all enclosed in a secure cabinet. While kiosks have existed since the late 1970s, only in the past few years has the kiosk market taken off. The dramatic increase in kiosk activity is the result of several factors.

Declining costs of microprocessors, printers, and other computer-related kiosk components have resulted in dramatically reduced kiosk costs.

The popularity of ATMs paved the way for widespread acceptance of kiosks. The public is more comfortable now using kiosks in a variety of settings. The use of touch screens has enhanced the popularity of kiosks by making them operable even by people lacking computer experience.

Increased use of the World Wide Web has fueled the growth in kiosk installations, with many organizations installing Internet commerce kiosks that provide users with Internet access and online purchasing capabilities.

Depending on the number of units in a kiosk network, physical infrastructure and software are the major costs. In small networks of one to 10 units, system design and programming represent the highest costs. In systems of 100 or more units, hardware and maintenance are the big-ticket items. Public agencies have tried several solutions to mitigate the overall expense of kiosk projects, including spreading the cost over several agencies; partnering with private-sector companies that design, manufacture and operate Internet-enabled kiosk networks; charging local advertisers for program space; and charging user fees for transactional services, such as paying parking tickets, obtaining hunting licenses, renewing drivers' licenses and applying for license plates.

Organizations can provide superior customer service by offering patrons access to kiosks that answer routine questions or handle routine transactions. These organizations save on personnel costs by reducing their need for sales clerks and customer service representatives.

Kiosks can dispense information or accept payments 24 hours a day, seven days a week, minimizing the need for customer service personnel while increasing overall efficiency.

The kiosk not only brings convenience to constituents, but also eases the congestion in government offices.

Some challenges include:

- Reliability and the need for kiosks to run for long periods of time without crashing or being rebooted.
- Updating content on kiosks deployed at a large number of locations.
- Gathering data about how the kiosks are being used.
- Fixing problems when no on-site service staff is available.

Mobile: Cell Phones, Wireless, Radio Frequency Identification Devices (RFID) and Near Field Communication (NFC)

Other emerging payment technology devices are cell phones and Personal Digital Assistants (PDAs). With high adoption rates of such devices, the ability to conduct e-commerce transactions is becoming vital to consumers. This technology is gaining at such rapid rates it is now classified as “**mobile commerce**.”

Cell Phones and Wireless

Mobile payments are a point-of-sale payment made through a mobile device, such as a cellular telephone, a smart phone, a PDA or a computer using Wi-Fi or wireless. Since mobile payments use wireless channels, they are also called micropayments, wireless payments or m-payments. The two key requirements for the successful, sustainable growth of m-payments and m-commerce are:

- Infrastructure
- Standards

The infrastructure must be in place to facilitate the electronic payment for goods and services to a sufficient installed base of consumers. But, equally important is the availability of new and innovative services that can be offered across wireless channels. In the more realistic, business case-focused world of today, the two are inextricably linked.

Investment in infrastructure will not occur without the prospect of revenues. New services will not be developed unless there is the prospect that the infrastructure will exist to support the payment for those services. Therefore, a clear business case needs to exist for all parts of the value chain, before significant investment will occur. Today's competitive environment is driven by rapid technological developments. Nontraditional players who are equipped to exploit new opportunities are entering key markets. At the same time, progress in electronic communications has led to increased technical collaboration among experts across industries and countries to support international commerce.

A new trend has become apparent – the movement toward open standards and interoperability of systems. In particular, we are seeing a growing adoption of international standards and specifications produced by open industry consortia. More and more organizations are seeing the big picture – that by ensuring interoperability across solutions, services, and platforms, we can have a more significant impact on the payments industry than ever before.

A framework that allows for flexibility yet delivers interoperability will be the key to m-commerce success. The unbridled optimism that may have existed two years ago has been tempered with a new sense of business realism, which is also ensuring that we focus on the key issues to be solved.

Mobile Internet Protocol (IP) and Wireless Fidelity (WiFi) Platforms for Mobile Payments

Mobile IP for ITS solutions is an open standard, defined by the Internet Engineering Task Force (IETF), which is becoming dominant today as it allows a user to keep the same IP address, stay connected, and maintain ongoing applications while roaming between IP networks.¹⁰ Mobile IP is scalable for the Internet because it is based on IP – any media that can support IP can support Mobile IP. Mobility and networks while-in-motion are becoming dominant themes for the mobile industry.

Such systems are starting to take off in Japan, where wireless operator NTT DoCoMo has launched its payment system that uses cell phones swiped over compliant point-of-sale terminals to make payments. So far, nearly 20,000 merchants are using the system in Japan.

Mobile payment seems likely to take off as a convenient way of paying for small items without going to a cash machine. But there could be risks in using them for larger items. Already people have been killed for their mobile handsets and if they contained stored credit, this might become more common. Fingerprint identification on phones may also not be much of a protection. Presumably it means the thief would have to kidnap the owner as well as the phone in order to spend the money on it.

The Capitol Corridor Joint Powers Authority (CCJPA), working with the state of California (Caltrans Rail Division), is running trials to lead an evaluation process for WiFi on-board the Capital Corridor trains with features for online usage and ability to support the utilization of the on-train and/or station wireless networks to support applications pertinent to train operations like e-ticketing¹¹

The ABI study noted that trials have shown that such systems can reduce so-called consumer pain points by making payments faster and reducing time in lines. The study cited multiple announcements that the various players are now aligned and wireless payment systems are ready to take off.

RFID and NFC

Two contactless technologies are contributing to the emerging channel of mobile government. RFID (Radio Frequency Identification Devices) and NFC (Near Field Communication) both represent opportunities in the government e-payment space.

¹⁰ <http://www.glocol.net/projects/train.html> This reference describes a research framework for mobile IP.

RFID is a method of remotely storing and retrieving data using devices called RFID tags. An RFID tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Tollway authorities are using RFID to efficiently manage ground transportation systems, assets, and transactions. This technology is facilitating the electronic collection of toll transactions. For more information, see NECCC's newly released pamphlet "RFID – Government Decision Makers Guide to RFID."

NFC is for very short range two-way wireless connectivity, and is a short-range radio frequency (RF) technology that allows a reader to read small amounts of data from other devices or tags when brought next to each other. NFC is based on contactless and Radio Frequency Identification (RFID) solutions, which consist of a tag and a reader. The reader, when activated, emits a short-range radio signal that powers up a microchip on the tag, and allows for reading a small amount of data that can be stored on the tag. NFC is different from other contactless or RFID technologies in that it has a very short operating distance and also allows two devices to interconnect. It is estimated that in the near future, this technology will surface in many ways; embedded into ID cards, passports, credit cards, and cell-phones to securely identify us for the purpose of granting access to and payment for services. If this technology is embedded in cell phones, instead of using your credit cards to pay for your tickets, gasoline, soft drinks or office supplies, your cell phone will be the single method of payment, making it your wallet of the future.

Matrix of Payment Channels and Payment Types

The following chart will help governments understand the variables they must consider when moving to electronic payments. Multiple payment channels can be used to address various constituencies. For example governments moving customers to Internet-based transactions have frequently added kiosks to address the concerns of citizens without access to the Internet. The horizontal axis identifies the various payment channels discussed in this paper.

Various payment channels offer a variety of benefits to the government accepting the payment as well as the consumer. These various bundles of services have different cost associated with them and some are limited to certain payment channels. The vertical axis identifies the payment types and the relative cost of these types to each other. A "✓" indicates that the payment type is universally accepted through that payment channel. The word "varies" indicates that the payment channel/type combination may be limited to certain banking networks and is not universally available across the United States and, therefore, all cards of a certain payment type may not work.

¹¹ *ibid*

Payment Channels

Payment Type	Acceptance Fees	Point of Sale	Telephone	Internet	Kiosk	Wireless
Cash or Check	None	√				
Credit Cards	High	√	√	√	√	√
Signature Debit Cards	High to moderate	√			√	
Pin-Less Debit Cards	Moderate		√	varies	√	varies
PIN-Based Debit	Low	√			√	
ACH	Low	√	√	√		√
Stored Value Cards	Low	√			√	
Digital Cash	Moderate	√	√	varies	varies	varies

Appendix A: Security Requirements for Payment Systems

Objective	Requirement
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	1. Protect stored cardholder data. 2. Encrypt transmission of cardholder data and sensitive information across public networks.
Maintain a Vulnerability Management Program	3. Use and regularly update antivirus software. 4. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	5. Restrict access to data by a need-to-know basis. 6. Assign a unique ID to each person with computer access. 7. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	8. Track and monitor all access to network resources and cardholder data. 9. Regularly test security systems and processes.
Maintain an Information Security Policy	10. Maintain a policy that addresses information security.

Common Vulnerabilities in the IT Structure

System Component	Potential Vulnerabilities
Network Firewall	Open ports for VPNs, Web access, remote employee access
Network Routers / Gateways	Misconfigurations, utilizing default passwords
Hosting Operating Systems	Known bugs, out-of-date patches, poorly defined and lax root access controls
Applications	Known bugs, viruses, Trojans
Data-Access Controls	Newly created databases, no separation of duties between administrators and users, employees separated from the company

Appendix B: Merchant Compliance Requirements

Compliance Level	Qualification Criteria	Compliance Requirements	Compliance Date
Merchant Level 1	Any merchant processing over 6 million credit card transactions annually.	- Annual on-site PCI DSS audit - Quarterly security perimeter scan conducted by DSS certified vendor	June 30, 2004
Merchant Level 2	Any merchant processing 150,000 to 6 million credit card transactions annually	- Annual self-assessment questionnaire filed through DSS certified vendor - Quarterly security perimeter scan conducted by DSS certified vendor	June 30, 2005
Merchant Level 3	Any merchant processing between 20,000 and 150,000 credit card transactions annually	- Annual self-assessment questionnaire filed through DSS certified vendor - Quarterly security perimeter scan conducted by DSS certified vendor	June 30, 2005
Merchant Level 4	All other merchants	- Annual self-assessment questionnaire recommended - Annual security perimeter scan recommended	Not applicable

Appendix C: Parties Involved in Stored Value Card Management

Stakeholder	Program Role
Issuing Financial Institution	• Management of Pooled/Aggregated Funds – Issuer is responsible for managing the funds on deposit according to applicable laws and network rules, including settlement and monitoring of cardholder transactions. • Liaison to Networks – As a member of the regional/international debit or credit network, the financial institution has the responsibility to complete all program administration and reporting, and assume all financial liability. • Advisory – The FI provides benefit of their experience with card-based products in the design of cardholder marketing, terms and conditions, dispute resolution, training and program launch.
Processor	• Cardholder account setup. • Card issuance and replacement. • Payment deposits to individual cards. • Transaction processing – including authorization, settlement and reconciliation. • Fraud monitoring and reporting. • Customer service to assist clients in managing card account.
Beneficiary Cardholder	• Responsible card use – adherence to program rules and procedures. • Reporting of lost or stolen cards.
Merchant (government)	• Acceptance of cards in accordance with network operating rules. • Timely processing and settlement of transactions. • Compliance and adherence to all security standards to protect cardholder information.

Payment Network	• Establishment and enforcement of rules and standards regarding issuance and acceptance of card. • Switch, report and settle transactions. • Enhance brand equity to benefit all parties in the payment transaction. • Review programs to ensure appropriate compliance and risk mitigation.
-----------------	--

Acknowledgements

Martin Benison, Office of the State Comptroller, Massachusetts – Work Group Co-Chair
Carolyn Purcell, Cisco Systems – Work Group Co-Chair

Steve Allison, Office of the State Comptroller, Idaho
Paul Benedetto, Department of Motor Vehicles, California
Cynthia Black, Vice President, MasterCard
Dan Combs, Global Identity Solutions
Lisa Counts, General Manager, NIC
John Cox, Bank of America
Dina Desiderio, NYC Department of Finance
Jaime Hill, NACHA
William Kilmartin, Accenture and NECCC Board Liaison
James Lock, JPMorgan Chase
Raymond McCabe, MADTA
Greg Miller, Office of Budget and Management, Ohio
Pam Valencia, Office of Financial Management, Washington
Lisa VanLaanen, Office of the State Controller, Oregon
Harsh Verma, GLOCOL, Inc.