Spring 2011 • No. 9

Debit Card Fundamentals and Their Use in Government Programs

By Cathy Corby Parker, James Wironen, Mollie G. Murphy, and Kevin J. Mahoney

The Community Living Assistance Services and Supports (CLASS) Plan – a groundbreaking component of the Affordable Care Act – creates a voluntary federally-administered insurance program to help individuals pay for needed assistance in a place they call home if they become functionally limited. Implementation will require knowledge translation from various sectors, including research and existing public and private programs. This Technical Assistance Brief Series seeks to answer questions pertinent to developing and implementing the program.

This brief describes the history and operation of debit cards and provides examples of their use in government programs to inform the use of debit cards to access CLASS Plan benefits.

Introduction and a History of Debit Cards

A little over 50 years ago, banks introduced credit cards. The utility of these early credit cards was limited as a payment card and would only work if both the merchant and consumer used the same bank. To address this issue, major banks formed franchises so that one bank's card could be accepted at another bank's merchant. These franchises became known as "associations." Today, Visa® and MasterCard® are the largest card associations and their product offers have expanded beyond credit cards.

Card associations play an important role in establishing the rules that govern use of payment cards by consumers and businesses. To protect the safety and integrity of the card-based payment system, all payment cards must be issued or guaranteed by a financial institution, and each merchant must be sponsored into the association by a financial institution.

Debit cards were introduced in the 1980's in the form of Automated Teller Machine (ATM) cards that provided consumers with 24-hour access to cash in their bank, checking, and savings accounts. A "debit card" is a plastic payment card that resembles a credit card but it is linked to the card owner's deposit account at a bank. When the card is used, it accesses funds the card owner has in his or her bank account. A Personal Identification Number (PIN) is associated with each debit card to protect against unauthorized use. To increase convenience for consumers, banks formed networks and allowed their customers to use ATMs owned by any bank in the network. A network logo was added to the card for consumers to easily identify the ATMs that were in the network. To extend the value of their ATM cards, networks encouraged merchants to install PIN-pads at their cash registers so consumers could make purchases with ATM cards. Over time, ATM cards came to be known as "debit cards."

In the 1990's, Visa and MasterCard launched their own version of debit cards that did not require use of a PIN for purchases. Instead, the consumer signed the back of the debit card and this signature could be matched with the consumer's signature on the receipt to validate the cardholder. Today, most debit cards operate in both modes, carrying one or more network brands and an association brand, allowing purchases to be authorized either with a PIN or the cardholder's signature.

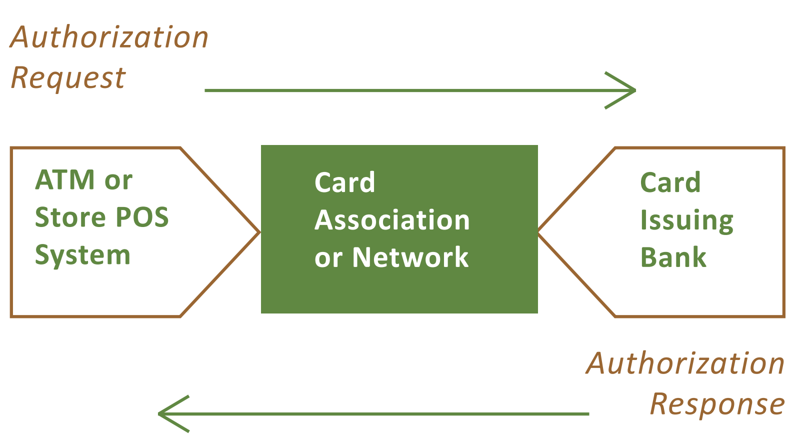
"A 'debit card' is a plastic payment card that resembles a credit card but it is linked to the card owner's deposit account at a bank. When the card is used, it accesses funds the card owner has in his or her bank account."

Originally, debit cards were linked to one or more bank accounts owned by the cardholder. Around the year 2000, a new form of debit card called a "prepaid debit card" was launched. The funds on prepaid cards were still kept at a bank, but in a pooled account where the balance was held in trust for cardholders. Behind the scenes, balances on each card were tracked in real time so that any one cardholder only had access to the funds in the trust account associated with his or her prepaid debit card.

How Debit Cards Work

When a consumer uses a debit card to get cash from an ATM or make a purchase, the ATM or merchant Point of Sale (POS) system sends an electronic request to the association or network linked to the card. The association passes the authorization request to the bank that provided the debit card to the consumer. The bank validates that the card has not expired or been reported lost or stolen and that there are sufficient funds available to cover the amount of the transaction. If a PIN is entered for identification, the PIN is also validated. The bank then sends the approval or denial transaction back to the association or network, who delivers it to the ATM or POS where the cardholder presented the card. (See Figure below.)

FIGURE Authorization Processing Transaction Flow



All of this happens nearly instantaneously – sometimes in less than one second of time. And, throughout the authorization process transactions are monitored to look for patterns of fraud.

"The newer debit card processing platforms associated with prepaid debit cards were designed to handle more complex authorization procedures. This could include limiting use of the card to certain categories of merchants or particular merchant locations. It could also include restricting use of the card to purchase of particular products or services if the merchant is able to send information about the items being purchased."

The newer debit card processing platforms associated with prepaid debit cards were designed to handle more complex authorization procedures. This could include limiting use of the card to certain categories of merchants or particular merchant locations. It could also include restricting use of the card to purchase of particular products or services if the merchant is able to send information about the items being purchased. Prepaid debit cards can also have multiple "purses" associated with a single card. For example, a prepaid debit card could have a general spending purse and a savings purse.

Debit Card Characteristics

There are a wide variety of debit card products in the market. Underlying this variation are five debit card characteristics that define the capabilities and uses for a debit card. These are:

- **Open Loop vs. Closed Loop** — "Open loop" means that the debit card is connected to an association or network and the card can be used at any merchant in the association or network. "Closed loop" is the term used for debit cards that are issued by a particular retailer and can only be used for purchases at that particular retailer. The most common closed loop cards are store gift cards. Some debit cards are hybrids of open loop and closed loop, in that they have a network or association brand, but they do not work at all merchants where that brand is accepted.
- **Reloadable vs. Non-Reloadable** — Reloadable prepaid cards operate very much like a bank account and the card issuer must validate the identity of the cardholder in essentially the same process as if the consumer was opening a bank account. Money can be loaded onto a reloadable card via direct deposit of pay or government benefits (the same as if the employer or government agency was depositing funds to a bank account). Consumers can also load money onto their cards at retail locations that participate in a reload network (such as GreenDot® or MoneyGram®) by giving cash to the retail store clerk to load onto the card. Non-reloadable prepaid cards are not associated with an individual. Because of their anonymous nature, there are strict limits on the dollar amount of funds that can be loaded onto a non-reloadable card.
- **PIN and/or Signature** — Debit cards can be issued with PIN and signature cardholder authentication, just PIN, or just signature. When a PIN is used, the card is processed over a network and the transaction is considered final at the time the authorization is approved. When a signature is used, the authorization is routed through an association, but the merchant must send an end-of-day electronic file to the association with all of the day's authorized transactions before the movement of money will occur. Cards that allow ATM access must have a

“Debit cards can be issued with PIN and signature cardholder authentication, just PIN, or just signature. When a PIN is used, the card is processed over a network and the transaction is considered final at the time the authorization is approved. When a signature is used, the authorization is routed through an association, but the merchant must send an end-of-day electronic file to the association with all of the day’s authorized transactions before the movement of money will occur.”

PIN. Many retailers allow customers to obtain cash back with purchases when a PIN is used. Cards that only use PINs are not able to be used for e-commerce purchases or bill payments at merchant web sites.

- **Registered or Anonymous** — All reloadable cards must be registered to a particular individual. Consumers with non-reloadable cards can register the card or use it anonymously. The advantage of registering a non-reloadable card is that it can then be used to make e-commerce or telephone purchases. Many online merchants will not accept unregistered cards because of the high risk of fraud.
- **Primary or Companion Card** — Both bank account-based and prepaid debit cards can have more than one card linked to a specific account. Two cards can both access the same funds or each card can have its own balance. Bank account-based debit cards have one balance shared by the primary and companion cards. Prepaid debit cards can operate similarly, but they can also be set-up to allow the primary cardholder to transfer funds to the companion card. In that case, each consumer has access only to the funds on his or her card, not the combined balance.

Common Debit Card Products

By varying the combinations of these five card characteristics, debit card providers have created dozens of different debit card products to meet specialized market needs. However, the most widely used debit cards fall into seven categories, each of which is highlighted below.

- **Bank-Account Based Debit Cards** — Today, virtually every checking account comes with a debit card. Most bank-based debit cards have both a signature and PIN. The number on the bank debit card is linked to one or more bank accounts. A purchase or withdrawal using a bank account-based debit card may be approved if there are not sufficient funds in the account, based upon the bank’s overdraft policies. Funds in the account associated with the bank debit card are insured by the Federal Deposit Insurance Corporation (FDIC).
- **Government Benefit Cards** — State and local government agencies spend millions of dollars annually printing and mailing checks to benefit recipients for programs such as Social Security, unemployment, and court ordered payments. To reduce costs and increase convenience for recipients, government agencies have encouraged direct deposit of benefits to recipients’ bank accounts. But, the FDIC estimates that in the U.S. 17 million people reside in households without bank accounts and another 21 million people have a bank account but conduct most of their financial business with cash and money orders.[1] This segment of the population uses check cashing services, where they can receive their funds in cash immediately without any hold period, as may be the case with a bank. To drive costs out of delivery of government payments to unbanked and underbanked consumers, many agencies have distributed reloadable prepaid debit cards to recipients who do not specify a bank account for direct deposit. These debit cards allow benefit recipients to withdraw their funds at an ATM or bank teller, and to make purchases in

stores and online. Government agencies work with the debit card providers to ensure that costs for the recipient are low. Recipients are usually allowed one free withdrawal after each deposit of benefits, and government benefit cards participate in at least one "surcharge-free" ATM network. "Surcharge-free" ATM networks allow cardholders to withdraw funds at an ATM without any fee from the owner of the ATM. While fraud does occur with government debit cards, as discussed later in this paper, the incidence and customer impact of debit card fraud is substantially lower than with check-based distribution of benefits. While comparable statistics are not available, paper checks are subject to being lost, stolen, or altered; there is no real-time authorization for paper checks, as with debit cards; and there are no consumer protections associated with use of checks.

- **Employee Payroll Debit Cards** — Employers for decades have promoted direct deposit of pay to bank accounts in order to save the expense of producing and distributing paychecks. Many employers now provide reloadable prepaid debit cards to employees who do not specify a bank account for direct deposit of their pay. These payroll debit cards have evolved into "checkless checking" accounts. Employees can deposit pay from multiple employers to these cards or even keep their cards when they change jobs. In many states, employers can mandate use of a payroll debit card for employees who do not specify a bank account for direct deposit, but they must provide the cards free, with no monthly fees and at least one free withdrawal after each payroll deposit. Employers have no ability to see card balance or transaction information on payroll debit cards.
- **General Purpose Reloadable (GPR) Cards** — As their name suggests, GPR cards are reloadable prepaid debit cards that can be purchased by consumers for a variety of uses. Consumers who don't have a credit card or bank debit card often use GPR cards to make purchases in stores and pay bills more conveniently than using cash or money orders, as well as for making purchases and paying bills online. Some consumers have their pay deposited to the GPR card – in essence, the GPR card becomes their bank account. Fees for GPR cards vary widely and can include a fee to purchase the card, a monthly maintenance fee and reload, ATM, and purchase transaction fees.
- **Flexible Spending Account (FSA) Cards** — Open loop prepaid cards linked to flexible spending accounts allow in-store and online purchases directly from the funds in the FSA – consumers do not have to file claims for reimbursement. FSA cards use signatures for authentication and do not have PINs or ATM access. Use of FSA funds is restricted to purchases of approved medical and healthcare products and services. Funds in the FSA cards are legally the property of the plan administrator and can only be loaded to the card by the plan administrator. FSA's operate on a "plan year" and at the end of the plan year, FSA administrators zero-out any remaining balances on the FSA card.
- **Health Savings Account (HSA) Cards** — HSA's are savings accounts associated with high deductible

insurance plans. An employee participating in a high-deductible insurance plan can open an HSA account at a bank and either the employee or employer deposits funds to the HSA. These funds earn interest tax-free and the funds can be used for out-of-pocket medical costs. At this time, there is no requirement that HSA account providers substantiate that the funds are used for medical purposes, and employees can withdraw their health savings funds in cash through an ATM or bank teller.

- **Gift Cards** — Gift cards are non-reloadable prepaid cards that can be either open loop or closed loop. The only way funds on a gift card can be accessed is to make purchases. Open loop gift cards can be used anywhere the association brand is accepted. Closed loop gift cards can only be used at stores owned by or affiliated with the retailer who issued the card (for example, a Home Depot® gift card is accepted only at Home Depot stores or the Home Depot web site). Gift cards can have a predetermined fixed balance or they can have variable funding with the card purchaser specifying the amount at the time of purchase. Because gift cards do not require registration, banks place limits on the maximum value that can be loaded onto a card to prevent the use of gift cards in money laundering.

The table on page 7 summarizes the features and characteristics of each of these major categories of debit cards.

Debit Card Providers

There is an "issuing bank" or "issuer" for every open loop bank or prepaid debit card. The bank has a fiduciary responsibility to the associations and networks in the case of fraud or misuse of the card, and is responsible for complying with association and network rules and government regulations. There is not a bank issuer associated with closed loop cards.

"Processors" are companies that process debit card transactions, acting on behalf of issuing banks to manage debit cards and authorize and settle transactions. Open loop card processors accept authorization requests from the associations or networks and approve or deny each transaction. On a daily basis, processors settle with the associations and networks to determine how much money each issuing bank owes each association and network for transactions approved for its cardholders. With closed loop cards, the retailer sends authorization requests directly to its card processing system or provider. There may be settlement involved if a card is purchased in one location of a chain or franchise store and redeemed in another location.

Processors also provide customer service to cardholders, including automated telephone access to account information and balances, an online cardholder web site and telephone agent customer service. Particularly in the case of government benefit programs, the cost of providing agent customer service can be unmanageable if cardholders are not sure how or where to use the card, or if

TABLE Summary of Characteristics of Widely Used Debit Card Products

	Bank Account Based Debit Cards	Payroll Debit Cards	Government Benefit Cards	General Purpose Reloadable Cards	Flexible Spending Cards	Health Savings Account Cards	Gift Cards
Account-Based or Prepaid	Account	Prepaid	Prepaid	Prepaid	Prepaid	Account	Prepaid
Open- or Closed-Loop	Open	Open	Open	Open	Open	Open	Open or Closed
Reloadable	N/A	Yes	Yes	Yes	Yes	N/A	No
ATM Access	Yes	Yes	Yes	Yes	No	Yes	No
Type of Authentication	PIN & Signature	PIN & Signature	PIN & Signature	PIN & Signature	Signature	PIN & Signature	Signature
Registered to Individual	Yes	Yes	Yes	Yes	Yes	Yes	Optional
Bank Identity Validation	Yes	Yes	Yes	Yes	No	Yes	No
Companion Card	Optional	Optional	Optional	Optional	No	No	No
Cardholder FDIC Insurance	Yes	Yes	Yes	Yes	No	Yes	No
Dispute Protection	Government & Association	Government & Association	Government & Association	Association Only	Association Only	Government & Association	Association Only
Funding Source	Consumer	Employer	Government Agency	Consumer	Employer	Employer or Employee	Consumer or Business
Owner of Funds	Cardholder	Cardholder	Cardholder	Cardholder	Employer	Cardholder	Cardholder
Funder Can See Balances/Activity	Yes	No	No	Yes	Yes	No	No
Direct Deposit of Pay	Yes	Yes	No	Yes	No	No	No
Reload Networks	N/A	Optional	No	Yes	No	N/A	No
Surcharge-Free ATM Network	Yes	Yes	Yes	Optional	No	Yes	No
Overdrafts Allowed	Optional	Optional	No	Optional	No	No	No

they are confused about whether their question should be directed to the card provider or the government agency. Clear communication in the collateral accompanying government benefit cards to minimize calls to customer service agents is critical.

"Banks, associations, networks, and processors have created an extensive infrastructure to protect the safety and soundness of the card payment system. There are detailed rules with which every member of an association or network must adhere, as well as government regulations."

Retailers sell prepaid debit cards to consumers either in stores or online. Generally, the cards sold in this way are open loop and closed loop gift cards or general purpose reloadable (GPR) cards. A "card mall" is often used to display an assortment of prepaid cards. Online card malls exist as well. Retailers that sell GPR cards generally also participate in prepaid reload networks and consumers can load funds onto reloadable prepaid debit cards in their stores.

Check cashers, payday lenders and money transfer agents often provide GPR cards to their customers. A portion of funds from cashing a check or loans proceeds can be applied to the GPR card to provide customers with the convenience of paying with plastic and the safety of not carrying around as much cash.

Mitigating the Misuse of Debit Cards

Banks, associations, networks, and processors have created an extensive infrastructure to protect the safety and soundness of the card payment system. There are detailed rules with which every member of an association or network must adhere, as well as government regulations.

PIN numbers have always been treated as highly sensitive by banks and never stored "in the clear" – meaning they were always encrypted when stored or in transit. More recently, the Payment Card Industry (PCI) Data Security Standard was established by the card associations to combat theft of the 16-digit credit and debit card numbers and associated cardholder names and card expiration dates. PCI compliance requires that any company that processes, stores, or transmits personally-identifiable payment information must maintain a secure environment. Issuers and processors are required to have annual third party audits to certify their compliance with PCI standards in order to maintain their memberships in the associations. Some states have adopted laws requiring compliance with data protection rules substantially similar to PCI requirements.

The Treasury Department and the Financial Crimes Enforcement Network developed regulations, as required by Section 326 of the Patriot Act, to maintain "Customer Identification Programs" (CIP) to protect against use of debit cards by terrorists. These regulations require that financial institutions verify the identity of the person opening a bank account and check to make sure that individual is not on the government's list of suspected terrorists.

To combat fraud through identity theft, the Federal Trade Commission (FTC) implemented the "Red Flags Rule" implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. "Red Flags" requires card issuers to diligently protect their

"Friendly fraud occurs when a family member or friend uses the card without the permission or knowledge of the cardholder. Friendly fraud can be especially serious if the cardholder has disclosed his or her PIN to a third party, as that individual can then use the card and PIN at an ATM to withdraw all the money in the account. This type of fraud is more common with government benefit and payroll debit cards, as the recipient population is less likely to have experience with debit cards. It is imperative that messaging to consumers that accompanies debit cards clearly communicates the importance of keeping the card secure and not disclosing the PIN to anybody."

cardholders from identity theft. In the debit card world, the focus is on fraud around address changes. A common scam is for a criminal to acquire a card number and cardholder name (for example, a server in a restaurant who takes the card out of view of the cardholder during the authorization process). Then the criminal calls the bank to change the address on the card and later reports the card lost or stolen. Thus the replacement card, when mailed, is sent to the criminal. Banks and processors now have policies to monitor and validate cardholder address changes. Generally, banks will contact the cardholder to validate the address change or request proof of the change, such as a copy of a utility bill.

Another risk with debit cards is "friendly fraud." Friendly fraud occurs when a family member or friend uses the card without the permission or knowledge of the cardholder. Friendly fraud can be especially serious if the cardholder has disclosed his or her PIN to a third party, as that individual can then use the card and PIN at an ATM to withdraw all the money in the account. This type of fraud is more common with government benefit and payroll debit cards, as the recipient population is less likely to have experience with debit cards. It is imperative that messaging to consumers that accompanies debit cards clearly communicates the importance of keeping the card secure and not disclosing the PIN to anybody.

An additional area of protection against fraud relates to loading of funds on the cards. Banks and processors monitor deposits to debit cards to assure that they are from corporate entities, other banks, government agencies or reload networks, or the cardholder herself/himself in the case of bank debit cards. The assumption is that these entities have performed due diligence on the businesses or individuals from whom they are accepting funds for deposit onto debit cards.

Cardholder rights in the case of disputes between the cardholder and the merchant are governed by association and network rules for open loop cards. Visa and MasterCard offer zero liability to protect cardholders against unauthorized charges as long as the cardholder promptly notifies the issuer.

The Federal Reserve also regulates open loop debit cards through "Regulation E" that limits the cardholder's liability for unauthorized purchases or ATM withdrawals to $50.00, as long as the customer promptly informs the bank.[2] At this time, Regulation E only applies to bank account-based debit cards and prepaid payroll and government benefit cards, although some GPR card providers extend the benefits of Regulation E to their customers. When a cardholder reports a dispute, the amount of the disputed transaction must be immediately credited back to the cardholder. Losses can occur with false filing of disputes if, upon resolution of the dispute in the merchant's favor, there are not sufficient funds to repay the credit that was extended to the cardholder. However, since both government benefit and payroll debit cards have recurring deposits, often the losses are recovered upon the next deposit to the card.

"Processors, associations, and networks continually scan authorization requests to look for patterns that indicate fraudulent activity. These systems are complex neural networks in which the financial services industry has invested billions of dollars. Fraud monitoring takes place at every level in the process, looking for abnormalities in the activity of the card account itself, the bank's card portfolio, the processor, the association or network, the merchant's processor, and the individual merchant."

Regulation E protects cardholders against friendly fraud if the cardholder reports it. However, cardholders are sometimes reluctant to report the fraud as many card issuers require the cardholder to file a police report that would implicate their "friend." Regulation E also requires financial institutions to send cardholders a monthly statement, which can be delivered electronically with the cardholder's consent.

There are no third parties protecting consumer dispute rights with closed loop cards. Any disputes with non-reloadable prepaid cards are resolved directly between the retailer and the cardholder.

Velocity limits associated with each debit card regulate the number and dollar value of activities that can be performed on a debit card. Each issuer establishes its own velocity limits and they vary by type of card program; however, common rules relate to the maximum daily cash withdrawal limit, maximum purchase value limit, and maximum dollar value of a prepaid debit card.

Processors, associations, and networks continually scan authorization requests to look for patterns that indicate fraudulent activity. These systems are complex neural networks in which the financial services industry has invested billions of dollars. Fraud monitoring takes place at every level in the process, looking for abnormalities in the activity of the card account itself, the bank's card portfolio, the processor, the association or network, the merchant's processor, and the individual merchant.

Debit Cards and Government Programs

Below are overviews of some of the major types of government and tax-preferred employee benefits debit card programs in use today.

Social Security Benefits — In 2008, the U.S. Treasury Department introduced Direct Express®, an open loop reloadable prepaid MasterCard. The new card allowed government benefit recipients without bank accounts to receive their benefits by direct deposit to the Direct Express card rather than a paper check. Social Security is the largest government program using Direct Express, but the card is also used for recipients of Supplemental Security Income, Veterans, Railroad Retirement and Office of Personnel Management Benefits. At the time the Treasury Department launched the Direct Express card, there were an estimated 4 million Social Security recipients without bank accounts. The Treasury Department projected savings would exceed $300 million in the first five years alone from depositing benefit payments to Direct Express cards rather than printing and mailing checks.[3] Use of Direct Express is voluntary for benefit recipients. However, in April 2010 the Treasury Department announced that as of March 2011, electronic deposit of benefits (to either a bank account or the Direct Express card) will be required for new benefit recipients and all existing recipients receiving paper checks must convert to electronic deposit by March

2013.[4] The Direct Express card has a fee structure that allows benefit recipients to use the card at little or no cost. The card is delivered to benefit recipients free of charge, has no monthly maintenance fees, no charge for customer service, and allows one free US-based ATM transaction after the monthly deposit of benefits. Additional ATM withdrawals cost recipients 90-cents.[5]

Unemployment Benefits — In the same search for cost reduction and efficiencies that fueled the US Government's introduction of Direct Express, many state governments have launched their own government benefit cards for payment of unemployment insurance and other state benefit programs. In 2009, an estimated $23 billion in unemployment benefits were distributed unto prepaid cards, and by mid-2010 every heavily populated state except for California had either launched or was in the process of introducing an unemployment claims payment card.[6] There are several different providers of these cards, and the particulars of the programs vary from state-to-state. However, the programs have in common that the cards are open loop, reloadable, with fee structures that allow recipients to use the card at little or no cost. While benefit recipients own the card, government agencies typically do not allow cards to be loaded with other than government funds. Recently, a handful of states have changed their positions and are allowing loading of cards with other than government funds; in essence, their benefit cards can serve as a checkless checking account even after the cardholder discontinues receiving benefits.

Court Ordered Payments — States are increasingly adopting open loop reloadable prepaid cards for delivery of court ordered payments. All of the savings associated with movement away from production and delivery of paper unemployment checks applies to checks for court ordered payments. Moreover, since court ordered payments are often delivering child support and/or alimony payments, emotions of the payer and/or recipient can be heated. Using open loop reloadable prepaid cards to deliver court ordered payments increases the transparency around payment and receipt of the funds. While judicial agencies at many levels in state governments administer court ordered payments, some states have adopted one prepaid debit card program for use by all judicial agencies within the state.

Food Stamps — Food Stamps were the first government benefit program to move to paperless benefit delivery, as the fraud associated with paper food stamps was high. By 2009, 36 states had implemented electronic benefit programs for foods stamps and all the rest were in the process of planning implementations.[7] Merchants participating in food stamp programs are required to validate that each item purchased is food stamp eligible. Prepaid debit technology, as we know it today, did not exist when the first EBT programs were launched. As a result, the financial services and merchant community invested in a new technology infrastructure called Electronic Benefit Transfer (EBT). New EBT networks were created, new cards were issued to food stamp recipients, and new terminals were installed at merchant locations to support the more complex authorization requirements. Because of the costs of the dedicated equipment, merchants may only support EBT in one check-out lane in the store. Thus, food stamp recipients could be inconvenienced and potentially ostracized as the fact that they are paying with food stamp funds would be apparent to other shoppers. Today, many EBT programs are retooling their EBT platforms to "mainstream" acceptance and processing of EBT cards with commercial payment card equipment and processes.

Flexible Spending Accounts — The federal government allows employers to offer Flexible Spending Accounts (FSAs) which let employees set aside pre-tax pay to fund out-of-pocket medical expenses. To prevent consumers from using these tax-advantaged funds for non-medical purchases, the government requires FSA plan administrators to substantiate the eligibility of each purchase. Consumers originally were required to submit a claim for reimbursement. This was inconvenient for consumers and limited the appeal to employees because FSA withholdings reduced net pay, then consumers put forth cash for the purchase and had to wait for reimbursement. In essence, FSA users were paying twice for the purchase before receiving their reimbursement. FSA cards addressed this issue by allowing consumers to access their FSA funds in stores via an FSA debit card. When FSA card issuers receive authorization requests, they must substantiate the medical nature of each item purchased. Issuers check the Merchant Category Code (MCC) sent in the authorization request, and deny transactions from non-healthcare merchant categories. Since large supermarket, discount, and drug stores sell both medical and non-medical goods, FSA cards cannot be accepted at these broad-based retailers unless the retailer distinguishes between eligible and ineligible purchases. Most of the large chains in these categories have modified their cash register systems to automatically identify which items are FSA eligible. These retailers maintain an Inventory Approval Information System (IIAS) that lists all the approved items for sale in the store or on an e-commerce site. At check-out, each item is matched against this list and a separate total is created for the FSA eligible and non-FSA eligible items. The consumer is allowed to pay for the qualified purchases from the FSA card and use another form of payment for ineligible items.

Considerations for CLASS Plan Design and Implementation

The Community Living Assistance Services and Supports (CLASS) provision in the Affordable Care Act requires that procedures be developed to allow use of debit cards to access cash benefits to be deposited into Life Independence Accounts.[8] This primer describes the history and operation of debit cards and provides examples of their use in government programs.[i]

[i] Additional considerations for integrating debit cards into CLASS Plan Design and Implementation are presented in The SCAN Foundation's CLASS Technical Assistance Series Brief #10: ("Financial Management Services in Participant Direction Programs"), Brief #11: ("Options for Getting Purchasing Power into the Hands of Participants: Lessons from Participant Direction Programs"), and Brief #12: ("Considerations for Debit Card and Cash Purchasing Mechanisms in the CLASS Plan").

Authors:

Cathy Corby Parker, M.B.A. is founder and President of Corby & Company, Inc., a Jacksonville Florida-based strategic consulting firm specializing in debit, prepaid and emerging payments.

James Wironen, M.B.A is the Director of Product Development & Consulting Services for the National Resource Center for Participant-Directed Services at Boston College, in Chestnut Hill, MA.

Mollie G. Murphy is the co-founder of Annkissam, a Cambridge, MA-based organization dedicated to building software tools for nonprofits. Mollie is also the Financial Management Services Expert Consultant at the National Resource Center for Participant-Directed Services at Boston College, in Chestnut Hill, MA.

References

1. Federal Deposit Insurance Corporation. (2009). *FDIC national survey of unbanked and underbanked households.* Washington, DC: U.S.Government Printing Office.
2. Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205 (2009).
3. United States Department of the Treasury Financial Management Service. (2008). U.S. Treasury introduces Direct Express® debit card for Social Security payments [Press release]. Retrieved fromhttp://www.fms.treas.gov/news/press/directexpress_launch.html
4. United States Department of the Treasury. (2010). Treasury goes green, saves, green broad new initiative will increase electronic transactions, save more than $400 million, 12 million pounds of paper in first five years alone [Press release]. Retrieved from http://www.treasury.gov/presscenter/press-releases/Pages/tg644.aspx
5. MasterCard. *Terms of use for your Direct Express® debit MasterCard® card.* Retrieved from http://www.usdirectexpress.com/edcfdtclient/docs/Terms_And_Condition.pdf
6. Mercator Advisory Group, Inc. (2010). *Seventh annual open loop prepaid market assessment.*
7. United States Department of Agriculture, Food and Nutrition Service. (2009). *EBT Alternatives Analysis.*
8. Patient Protection and Affordable Care Act, Pub. L. No. 111th-111-148, § 8002 (2009). Print.