Insolvency Risk in the Network-Branded Prepaid-Card Value Chain

Philip Keitel*

September 2011

Summary: *The value chain for network-branded prepaid cards involves more parties than those commonly present in credit- or debit-card-issuing arrangements: the merchant acquirer, processors, a payment network, and a card-issuing bank. These additional participants may include a program manager, a distributor, and a seller. Since a number of independent businesses make up the chain, each one, as well as cardholding consumers, could be exposed to losses resulting from the insolvency of another party in the value chain. This risk is both real and manageable, as illustrated by two recent incidents involving network-branded prepaid cards: the failures of Silverton Bank, N.A., and Springbok Services, Inc. The Payment Cards Center of the Federal Reserve Bank of Philadelphia hosted a workshop on March 18, 2011, to examine the implications of insolvency in the network-branded prepaid-card value chain, to review how market participants have responded to this risk, and to discuss controls the industry has developed to mitigate and address these challenges. Kirsten Trusko, president of the Network Branded Prepaid Card Association (NBPCA); Terry Maher, partner at Baird Holm LLP and general counsel to the NBPCA; Jeremy Kuiper, managing director of the Bancorp Bank; and Ted Martinez, head of Visa's North America credit settlement risk team, led the workshop. This paper summarizes the information presented at the workshop, including the ways in which consumers and businesses are protected from the insolvency of the issuing bank or a key participant. In addition, this paper highlights practices that have been developed in the industry to mitigate this risk.*

Keywords: Network-branded prepaid cards, general-purpose reloadable prepaid cards, electronic payments
JEL Classification Numbers: D14, D18, E42

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: philip.keitel@phil.frb.org.The views expressed here are those of the author and do not necessarily reflect the views of the Federal Reserve Bank of Philadelphia or the Federal Reserve System. This paper is available free of charge at www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/.

I. Introduction

On March 18, 2011, the Payment Cards Center of the Federal Reserve Bank of Philadelphia hosted a workshop to discuss insolvency risk in the network-branded prepaid-card value chain, and, in particular, whether the insolvency of a key participant in the value chain poses a threat to consumers and banks.[1] The potential effects of key-participant insolvency became apparent in 2009, following the insolvency of Silverton Bank, N.A.,[2] which provided prepaid-card-issuing services to client banks, and the 2010 insolvency of Springbok Services, Inc., a program manager.[3]

This workshop discussed potential insolvency issues that might arise with prepaid cards that are issued by banks and branded with payment networks' logos. It did not discuss issues that might arise for consumers with prepaid cards issued by a retailer that goes bankrupt.[4]

Kirsten Trusko, president of the Network Branded Prepaid Card Association (NBPCA); Terry Maher, partner at Baird Holm LLP and general counsel to the NBPCA; Jeremy Kuiper, managing director of the Bancorp Bank; and Ted Martinez, head of Visa's North America credit settlement risk team, led the workshop.

The presentations and discussions at the workshop made it clear that the insolvency of a participant in the prepaid value chain poses a potential risk to both

---

[1] Key participant, as it is used here, simply means a party integral to a particular prepaid card program. For example, an issuing bank or a program manager would be a key participant in a program.

[2] For more information, see Federal Deposit Insurance Corporation, "FDIC Creates Bridge Bank to Take Over Operations of Silverton Bank, National Association, Atlanta Georgia" (Washington D.C.: FDIC Press Release, May 2009).

[3] For more information, see Will Hernandez, "Springbok Bankruptcy Filing Might Signal Rough Times Ahead for Prepaid," *PaymentsSource*, June 28, 2010.

[4] In such instances, a prepaid cardholder typically becomes an unsecured creditor of the retailer. The retailer may continue to honor and service those cards, but it may have to obtain permission to do so from its outstanding creditors. See Adam Saytanides, "Cardholders' Fate Uncertain When Stores Go Bankrupt," *Prepaid Trends*, June 4, 2008, 3:11, pp. 1, 5, 11 & 12.

consumers and banks, but those risks can be managed and mitigated. Banks, payment networks, program managers, and other parties can use a variety of tools and strategies to protect themselves — and their customers — from risks posed by their business partners. There are also a variety of state and federal regulations, or regulatory guidance, that outline the duties of various participants in the prepaid value chain.

This paper is organized as follows. Section II provides background information on the network-branded prepaid-card industry, as well as a description of the insolvencies of Silverton and Springbok. Section III reviews protections available to consumers from the insolvency of a bank or a key program participant. Section IV explains the role of payment networks, paying particular attention to the role that networks play in establishing rules and providing protection to various parties. Section V examines how banks protect themselves from the risk that a business partner will become insolvent and how the industry has responded, overall, to insolvency risk. The final section concludes.

II. Background

Network-branded prepaid cards are payment cards that bear the mark of a payment network (Visa, MasterCard, American Express, or Discover, for example) and that access funds that a consumer or business has paid in advance.[5] In 2009, 1.3 billion noncash consumer payment transactions were made using prepaid payment instruments branded with either credit card or PIN networks. In recent years, the number of prepaid

[5] For more information on prepaid cards and how they work, see Julia Cheney and Sherrie Rhine, "Prepaid Cards: An Important Innovation in Financial Services," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper (2006), and Mark Furletti, "Prepaid Cards: How Do They Function? How Are They Regulated?" Federal Reserve Bank of Philadelphia Payment Cards Center Conference Summary (2004), available at: www.philadelphiafed.org/payment-cards-center/.

card transactions has been growing by more than 20 percent per year, which is more than twice the rate of payment card transactions as a whole.[6]

A. Structure of the Network-Branded Prepaid-Card Value Chain

As Kirsten Trusko of the NBPCA explained, prepaid cards differ from credit cards and debit cards in the types of funds they access and also with regard to the number of parties that play a role in getting cards into consumers' hands. Trusko observed that the network-branded prepaid-card value chain generally involves more parties than a typical debit- or credit-card-issuing arrangement. A typical debit-card- or credit-card-related value chain generally involves a card-issuing bank, an issuer processor, a payment network, an acquiring processor, and an acquiring bank. A network-branded prepaid-card value chain generally includes these parties as well as a program manager, distributor, and seller.[7]

Definitions

An issuer refers to a financial institution that issues the card to a consumer or business and that is a member of a payment network. An issuer's processor provides transaction processing for the financial institution and often provides customer service.

The network provides the infrastructure for authorizing, clearing, settling, and processing the transaction and also provides risk management services.

An acquiring bank is the bank that provides services to the card-accepting merchant. An acquiring processor provides card processing services for the merchant acquiring bank.

The program manager is a company that, under direct supervision and contract of the financial institution, designs and runs the card program and sometimes provides customer service.

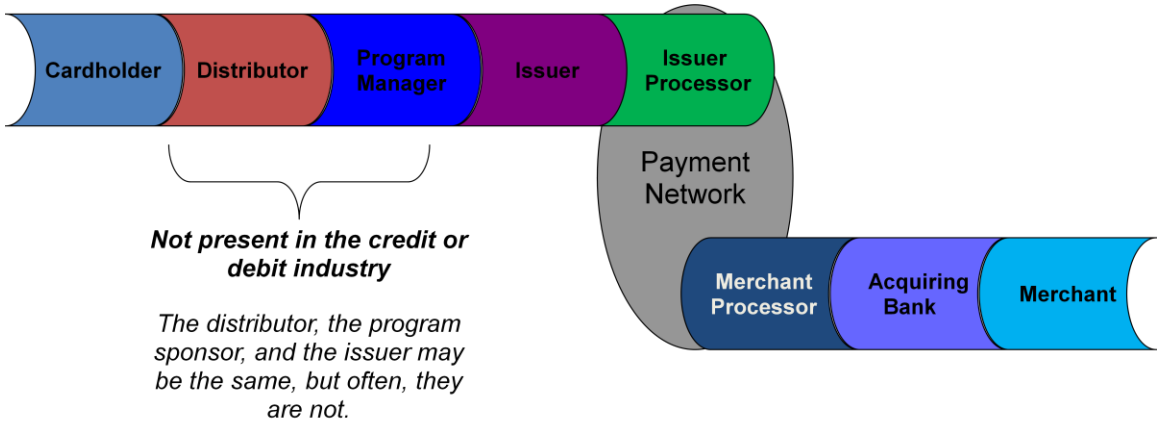
A distributor is responsible for shipping cards to endpoints. Sellers make cards available to consumers and businesses.

---

[6] The Federal Reserve System, *The 2010 Federal Reserve Payments Study: Noncash Payment Trends in the United States: 2006-2009* (December 2010), p. 17. The 2010 study is the Fed's most recent analysis of noncash payment trends in the United States.

[7] For more information on payment card processing in the United States, see Ann Kjos, "The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper (October 2007). And for more information about the role of program managers and other parties in the prepaid value chain, see John Yeomans, "Viewpoint: The Role of the Prepaid Program Manager," *Paybefore.com* (December 2010).

Basic Network-Branded Prepaid-Card Value Chain Graphic



Trusko noted that since a number of independent businesses make up the value chain, each one could be exposed to losses resulting from the insolvency of another party in the value chain. But she argued that the risks to these businesses, as well as any risk posed to cardholding consumers, are significantly diminished by consumer protections and industry practices (which are reviewed later on).

B. Recent Insolvencies Affecting Network-Branded Prepaid Programs

Such failures do happen. In May 2009, Silverton Bank, N.A., in Atlanta, Georgia, was closed by the Office of the Comptroller of the Currency after its capital position had deteriorated.[8] With regard to Silverton's closing, the FDIC specifically noted that Silverton "failed due to significant loan losses which eroded its capital position and reduced its ability to maintain adequate liquidity."[9] Although Silverton did not issue

[8] See Federal Deposit Insurance Corporation (May 2009), p. 1.

[9] See Federal Deposit Insurance Corporation, "Failed Bank Information: Question and Answer Guide for Silverton Bank, N.A., Atlanta, Georgia," at "Silverton failed: Why did Silverton, N.A. fail?", available at:

prepaid cards directly to consumers, it operated prepaid programs for other banks, supported those programs, and provided customer service related to those programs.[10]

To alleviate any concern that these programs would be interrupted, the Federal Deposit Insurance Corporation specifically addressed Silverton's prepaid card programs in communications to Silverton's client banks and in a question-and-answer format on the agency's website.[11] There, the FDIC noted that cards would continue to "have value" — consumers would be able to access underlying funds — and that settlement services and customer support services would be uninterrupted.

In 2010, Springbok Services, Inc., a program manager involved in a number of loyalty, promotion, and rewards programs and other prepaid programs, filed for Chapter 11. In its filing, the company cited cash-flow problems and high overhead (which caused expenses to exceed revenues) as the chief factors contributing to the firm's filing.[12] Although there were initial reports of cardholders being unable to access funds,[13] banks that worked with Springbok (acting as issuers for the cards in Springbok's programs) agreed to continue processing and servicing outstanding card transactions, providing

---

www.fdic.gov/bank/individual/failed/silverton_q_and_a.html (last updated February 2011) (accessed August 2, 2011).

[10] See Federal Deposit Insurance Corporation (February 2011) and Federal Deposit Insurance Corporation, "Failed Bank Information; Silverton Bridge Bank, N.A., Client Bank Conference Call," (May 2, 2009), available at: www.fdic.gov/bank/individual/failed/silvertonconference.html (accessed May 11, 2011), detailing the role that Silverton played in relation to prepaid card programs.

[11] See footnote 10.

[12] See "With Springbok, Fifth Third Gets into Open-Loop Prepaid," *Digital Transactions*, September 23, 2010, available at: www.digitaltransactions.net/news/story/2648, accessed August 2, 2011, summarizing the reasons for filing that Springbok cited in its bankruptcy filing and noting that "in January 2010 [ ] a client projected to account for 35% of [Springbok's] revenues, Group O Inc., terminated its Springbok prepaid card program," and that attempts to raise capital or sell assets prior to the firm's bankruptcy filing were unsuccessful.

[13] See, for example, Elizabeth Souder, "TXU Rewards Cards May Not Work," *The Dallas Morning News*, June 23, 2010, and Will Hernandez, "Springbok Creditors Line Up," *American Banker*, June 29, 2010.

cardholders access to their funds.[14] As creditors of Springbok, these banks, along with companies that had paid Springbok to provide their employees and customers with rewards and loyalty cards,[15] sought damages from the program manager. Ultimately, Sprinbok's prepaid-card-processing platform was sold to Fifth Third Processing Solutions, L.L.C. of Cincinnati.[16]

III. Insolvency Risk and Consumers

Terry Maher, of the law firm Baird Holm LLP, and general counsel to the NBPCA, discussed the implications for consumers when a party to the network-branded prepaid-card value chain becomes insolvent. As Maher explained, risks to consumers are mitigated by protections against key-participant insolvency derived from several sources, including (1) FDIC deposit insurance, (2) state money-transmitter licensing laws, (3) and underlying contracts between the various participants. Thus, while it is possible that a company in the network-branded prepaid-card value chain will become insolvent, the insolvency itself does not mean that a consumer will be harmed or that cardholders will be unable to ultimately access underlying funds.

A. FDIC Deposit Insurance

First, Maher drew attention to the FDIC's deposit insurance rules. He explained that when a bank that issues prepaid cards becomes insolvent, insurance proceeds in the

[14] See Hernandez (June 28, 2010).

[15] Companies such as Starz Entertainment, Nationwide Insurance, and Mercedes-Benz Financial.

[16] See Fifth Third, "Fifth Third Processing Solutions Expands Prepaid Card Processing Capabilities through Acquisition of Springbok Services, Inc. Prepaid Platform" (Cincinnati, OH: Fifth Third Press Release, September 21, 2010); and "Cincinnati Firm Buys Springbok Services Assets," *Denver Business Journal*, September 22, 2010.

amount of any remaining underlying funds (up to the current insurance limit) will be disbursed to the owners of those funds, so long as FDIC requirements have been met.

Under FDIC rules, holders of prepaid cards will be treated as owners of the deposits associated with those cards (the underlying funds associated with each card) and will therefore be entitled to insurance proceeds, as long as the FDIC's standard "pass-through" requirements are met.[17] These requirements are: (1) the agency or custodial relationship must be disclosed in the account records of the insured depository institution; (2) the identities and interests of the actual owners must be disclosed in the records of the depository institution or records maintained by the custodian or other party; and (3) the deposits must be owned (under the contract) by the named owners and not by the custodian. If insurance does not pass-through to the consumer, the card distributer, program manager, or other named account holder will be recognized as the owner.

FDIC insurance can be an important protection for users of some types of prepaid cards. In December 2010 the Treasury Department issued regulations that require prepaid programs that receive federal benefit payments from the Treasury Department (such as Social Security benefits) to pass through FDIC deposit insurance to the cardholder.[18] It has been suggested that this requirement by the Treasury Department may establish FDIC

[17] The rules that determine when deposit insurance extends to cardholders are contained in New General Counsel's Opinion No. 8. This new opinion, which was issued on November 8, 2008, replaces the previous General Counsel's Opinion No. 8 (released in 2006) and is available at www.fdic.gov/news/news/financial/2008/fil08129.html (accessed September 15, 2010).

[18] Federal Government Participation in the Automated Clearing House, 75 *Fed. Reg*. 80,335 (December 22, 2010).

insurance as a standard protection and may cause segments of the prepaid industry to routinely offer FDIC insurance to cardholders.[19]

In addition to the basic rules governing when FDIC insurance extends to prepaid cardholders, Maher highlighted protections contained in section 343 of the Dodd-Frank Act. This portion of the statute requires the FDIC to provide deposit insurance coverage for balances in non-interest-bearing transaction accounts, regardless of their size, from December 31, 2010 to December 31, 2012.[20] Thus, additional FDIC deposit insurance protection is available to consumers who use network-branded prepaid cards that have underlying structures that meet statutory requirements.

B. State Money-Transmitter Licensing Laws

Next, Maher discussed the effects of state money-transmitter licensing laws. As Maher explained, these laws often apply to at least one entity in the value chain (such as a card issuer or a program manager) and require safety and soundness reviews of applicants and licensees, as well as compliance with substantive provisions.[21] He noted that, in general, licensees must satisfy minimum financial standards, must post a surety bond (or

---

[19] See David Newville and Melissa Koide, "Prepaid Cards and Consumer Protections," a report issued by the Center for Financial Services Innovation, August 2011, p. 4, noting that most major providers of general-purpose reloadable prepaid card accounts are now formally offering FDIC insurance and other substantive protections to customers as a result of the Treasury Department's rulemaking.

[20] See Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111-203, Title III, Subtitle D, Section 343) (2010). Note that non-interest-bearing transaction account is defined as an account (1) with respect to which interest is neither accrued or paid; (2) on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone or other electronic media transfers, or other similar items for the purpose of making payments or transfers to third parties or others; and (3) on which the insured depository institution does not reserve the right to require advance notice of an intended withdrawal.

[21] See, for example, California's Money Transmission Act, available from the Money Transmitter Division of the Department of Financial Institutions, at: www.dfi.ca.gov/licensees/moneytransmitters/ (accessed May 13, 2011).

must provide some other form of security), and must maintain sufficient investments in permitted investment vehicles.[22]

Moreover, licensed money transmitters typically must submit periodic reports to state agencies and must allow inspection and examination. These exams typically focus on the safety and soundness of the institution, anti-money-laundering policies and procedures, management and oversight of relationships with agents of the firm, information security practices, and compliance with other state requirements. Maher pointed out that a byproduct of state supervision is that greater certainty about the resilience and practices of money transmitters benefits consumers who use prepaid products.

C. Contractual Obligations

Third, Maher explained that contracts that underlie the value chain can also protect consumers. As Maher detailed, cardholders always have contracts with issuing banks, and these contracts contain protections for the cardholders. In addition, cardholders also benefit from protections that result from obligations established by contracts between different parties in the prepaid value chain. For example, payment card networks have contracts with card-issuing banks and the acquiring banks. Card-issuing banks have contracts with program managers. Distributors, reload networks, selling merchants, and reload agents have contracts with card-issuing banks and/or program managers. And cardholders have contracts with card-issuing banks.

Each of these contracts may contain provisions that reduce the likelihood of a key participant's insolvency or its impact on consumers. For example, contracts between

[22] Maher observed that surety bonds can range in value from $25,000 to up to $1 million and are required in each state in which a licensed money transmitter does business.

banks and program managers often require that program managers have a reserve account at the issuing bank. Or they may limit the amount of time a program manager, or its agent, may hold funds loaded by a consumer before those funds must be remitted to the bank. These and other contract provisions (which are covered in more detail in Section V below) are designed to protect the issuing bank. But they also protect cardholders by ensuring that their funds are stored in FDIC-insured accounts.

As with contracts between card-issuing banks and program managers, contracts between payment networks and banks can also benefit cardholders. For example, payment networks typically require issuing banks to provide the network with up-to-date information on all program managers they do business with. By knowing how many banks do business with each program manager, payment networks can anticipate the potential impact of a single distressed program manager. This information about the interconnectedness of payment system participants can help to identify potential sources of system risk in a card-based payment system.[23]

Payment network contracts with banks also typically require that 100 percent of the underlying program's balances be held at a financial institution. This ensures that funds are on hand at the issuing bank when consumers use their cards. The role of payment networks is discussed in more detail in the next section.

As Maher highlighted during the workshop, consumers have several sources of protection from the potential effects resulting from the insolvency of a key participant in the network-branded prepaid-card value chain. Therefore, the overall effects of a key participant's failure on consumers can be limited, even if there are delays in consumers'

[23] The term system risk as used here should not be interpreted to mean risk to the financial system or to the economy. Rather, the term refers to the potential that mutual exposure to an important network participant might result in knock-on effects for other prepaid card programs.

ability to access funds while, for example, issuers, payment networks, and/or regulators respond.

IV. The Role of Payment Networks in Mitigating Insolvency Risk

Rules established by payment networks and, in particular, contracts between payment networks and banks establish many of the rules that govern the operation of electronic payment systems. They also contain important protections for banks and consumers.[24] Ted Martinez, head of Visa's North America credit settlement risk team, described the role Visa plays in the network-branded prepaid-card value chain, discussed how the company uses different strategies to help evaluate and limit risks posed by parties in the value chain, and highlighted one way Visa protects its member banks from insolvency risk — the settlement guarantee.

As Martinez explained, payment networks operate the infrastructure over which electronic consumer payments are authorized, clear, and settle. They facilitate the movement of settlement funds between card-issuing banks and merchant acquiring banks (member banks), provide processing and operational systems, set standards and rules for client banks (which include both issuing and acquiring banks), develop payment products, and provide risk management tools, such as monitoring transaction fraud.

[24] For research from the Payment Cards Center that highlights protections derived from payment network rules, see Mark Furletti and Stephen Smith, "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper (January 2005), pp. 12-16 & 25-29; and Mark Furletti and Stephen Smith, "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: ACH E-Checks & Prepaid Cards," Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper (March 2005), pp. 7-10 & 15-16.

A. Identifying Parties in the Value Chain

As central parties to a transaction, payment networks can be affected by the actions of their member banks as well as those of the many companies that provide services to banks, referred to here as agents or banks' agents. Martinez observed that an important first step to reducing and mitigating risk is to identify the parties in the value chain. Martinez explained that the Visa Third-Party Agent Registration Program is one way the network does this.

Under this program, the network gathers information about banks' agents by requiring member banks to register all third-party agents.[25] Failure to register a third-party agent may result in a fine by the network. This program helps develop an overall map of the firms involved in the authorization, clearing, and settlement of payment transactions and a means of identifying the potential effects of the failure of a particular firm.

B. Information Gathering and Due Diligence

The Visa Third-Party Agent Registration Program also requires that banks evaluate their agents' compliance with network rules. They must attest to having completed such evaluations, providing confirming documentation at the network's request. For example, member banks must perform an annual review of all third-party

[25] To Visa, an agent is any entity that is not directly connected to VisaNet (the network) and that, directly or indirectly, provides payment-related services to a Visa member, merchant, or third-party agent of a registered member, and/or stores, processes, or transmits Visa account numbers. Agents perform multiple functions on the issuing and acquiring side of a Visa member's business. Agents are generally classified by Visa as independent sales organizations (ISOs), encryption and support organizations (ESOs), third-party servicers (TSPs), or merchant servicers (MSs). Each function performed by an agent must be registered by each Visa member using those services. Agent functions that require registration include, but are not limited to, merchant or cardholder solicitation activities and/or customer service; prepaid program solicitation and/or customer service; deployment, servicing, and maintenance of an automated teller machine (ATM); deployment, servicing, and maintenance of a point-of-sale device; storing, processing, or transmitting Visa account numbers; and loading software or injecting encryption keys into ATMs, terminals, or PIN pads.

agents to confirm ongoing compliance with network-established due diligence standards. Some examples of due diligence include verifying that a third party is financially responsible and performing background checks of the principals. If noncompliance is found, Visa may impose fines or requirements related to specific third-party agents or those agents' actions or even prohibit a third-party agent from providing services to Visa clients.

Visa also gathers information (and imposes penalties for noncompliance with network rules and regulations) under its USA Prepaid Issuer Risk Program. Under this program, the network reviews prepaid-card-issuers' policies, procedures, and controls; agent agreements; sources of funding; monitoring of agents; and agent-to-cardholder communication and education in order to ensure that banks that issue prepaid cards adequately manage their relationships with agents that help support the operation of their prepaid card programs.

As Martinez explained, information gathered under the USA Prepaid Issuer Risk Program about business arrangements, banks' agents, and risks comes from two primary sources: self-assessment questionnaires that prepaid-card-issuing member banks must fill out and independent on-site reviews of issuers and agents that are carried out by, or on behalf of, the network. Visa then uses this information to determine if an issuer is in compliance with network rules. If an issuer is not in compliance, or if risks are identified, Visa may impose fines, limit the access that that issuer has to the network, or, in extreme cases, may terminate the relationship between the network and the member bank.

C. Possession and Control of Funds

Martinez explained that Visa, in its Operating Regulations, requires that 100 percent of a prepaid program's underlying balances be held and controlled by the card-issuing, Visa member bank. There are some exceptions to this rule, such as some programs that are designed under Internal Revenue Service regulations and that involve employers.[26] But, in general, this requirement calls for all funds related to prepaid card programs to be accessible to cardholders. Compliance with this requirement is verified through on-site reviews. If a member bank is not in compliance, Visa will work with that bank to ensure that it becomes compliant. Martinez explained that, to date, Visa has not had to impose controls to ensure that a particular member bank complies with this rule, but he noted that the network is able to impose fines, limit the access that the issuer has to the network, and terminate the relationship between the network and the member bank.

D. The Settlement Guarantee

Last, Martinez detailed a form of insurance that Visa provides to financial institutions to protect them from another financial institution's inability to meet its settlement obligations. This is what Visa calls the settlement guarantee. The settlement guarantee is an important source of protection for banks because it shields them from insolvency risk associated with other banks in the settlement scheme. (Interbank settlement typically occurs on the same day, or one day after, a transaction is cleared.) Without such a guarantee, banks might be less willing to participate in the network. And

[26] For example, flexible spending accounts and health savings accounts (HSAs) are exempt from this requirement. Notwithstanding this exception, on-site reviews performed by or on behalf of Visa assess the controls in place with these programs to ensure that they are sound and appropriate. For more information on FSAs and HSAs, see the Internal Revenue Service's website at: www.irs.gov (accessed June 30, 2011).

because Visa is providing this guarantee, it has an incentive to engage in the forms of monitoring and rule-setting described earlier in this section.

V. Risks to Banks (and Strategies for Mitigating Those Risks)

In the wake of Springbok's Chapter 11 filing, several banks found themselves unsecured creditors of the program manager, including KeyBank, which sought $15 million in damages, and MetaBank, which sought $3.4 million in damages.[27] As Jeremy Kuiper, of the Bankcorp Bank (a large prepaid-card-issuing bank), explained, this type of situation is not typical. According to Kuiper, prepaid-card-issuing banks today are well aware of insolvency risk and have built into their processes and practices many measures that protect them from business-partner insolvency (and from shocks related to business partners' agents coming under financial stress). He noted that as prepaid programs have become larger and larger, the industry's adoption of risk-mitigating practices reflects an increased awareness of issuing banks' exposure to risks.

A. The Good Funds Model

The primary protection for prepaid-card-issuing banks is something Kuiper called the good funds model. Under the good funds model, an issuing bank requires all underlying funds to be deposited at the bank *before* cardholders can use their cards. As with Visa's program-funding requirement, the good funds model requires rapid remittance to the issuing bank of any funds loaded on to cards by consumers. This reduces the amount of consumers' funds held by program managers, or their agents, and the amount of time they hold those funds. While similar to Visa's requirement that 100

[27] See Hernandez (June 28, 2010).

percent of funds be held and controlled by the card-issuing bank, the good funds model is distinct in that this requirement originates with the bank and applies to the bank's partners.

Kuiper mentioned that banks sometimes require program managers to fund a reserve account that exists independently from any underlying program account. He acknowledged that there are some programs that require special arrangements, such as flexible spending accounts,[28] but he argued that these exceptions are few, are typically lower-risk programs, and often involve a party, such as an employer, that is willing to pre-fund an account. Kuiper argued that, fundamentally, prepaid-card-issuing banks "are not in the business of making unsecured loans [to program managers]."

B. Other Risk Mitigation Practices

Kuiper noted that prepaid-card-issuing banks have developed many other processes and practices that mitigate insolvency risk in the value chain. He observed that banks: (1) provide detailed information to regulators and can (2) carefully evaluate business partners and their agents, (3) assess the financial risk of particular programs, (4) structure contracts to reduce risks, (5) institute strict oversight policies, (6) use licensed money transmitters for loads/reloads, and (7) structure accounts to provide the maximum amount of deposit insurance allowed under FDIC regulations.

First, Kuiper noted that prepaid-card-issuing banks are regulated entities, subject to frequent examinations by regulatory authorities. He observed that these examinations often focus on the bank's safety and soundness.

---

[28] Flexible spending accounts are tax-advantaged financial accounts that allow employees to set aside a portion of their pay for qualified expenses. Ultimately, these accounts are funded by remittances associated with periodic deductions from an employee's pay. However, to enable cardholders' expedient access to funds, employers often provide funds in advance of deductions from pay.

Second, Kuiper focused on what he called due diligence of related third parties. Essentially, as Kuiper explained, the careful evaluation of business partners and their agents helps reduce a bank's exposure to insolvency risk. In particular, Kuiper noted that reviewing financial statements of business partners and their agents, obtaining background checks on owners, creating contingency plans with business partners (in the event an agent becomes insolvent), conducting detailed reviews of partners' compliance with network rules and rules related to payment system operation (such as rules intended to limit payments fraud), and obtaining insurance coverage are all good protective measures banks can take. In addition, Kuiper noted that developing and refining comprehensive risk-assessment matrices, which can be used to evaluate potential business partners and their agents, can help identify and assess risks in advance.

Third, Kuiper argued that the particular risk-related characteristics of individual prepaid programs and the overall financial risk that a program poses should be considered by the issuing bank on a program-by-program basis. He explained that Bancorp uses a five-tier system to do this. He noted that higher-risk programs might receive enhanced financial monitoring and/or have reserve account requirements put in place.

Fourth, Kuiper stressed that contracts between banks and their business partners need to be structured to address insolvency risk. For example, it is possible to include in contracts clauses that: (1) clearly define the services that a bank's business partner is to provide; (2) prohibit a business partner from subcontracting without review and approval by the bank; (3) set compliance requirements (related to, for example, network rules, data security requirements, or regulations); (4) provide for the bank to have access to business partners' records; (5) craft performance requirements and standards; (6) set requirements

for periodic reports or audits; (7) require disclosure of complaints; (8) require indemnification for the bank in certain instances; and (9) include provisions that would trigger default and termination under the terms of the contract.

Fifth, Kuiper argued that prepaid-card-issuing banks must be vigilant in their oversight of business partners once programs are up and running. This means continual and proactive assessments to determine compliance. This is accomplished by, for example, periodically reviewing business partners' operations to ensure that they are consistent with the contract, as well as periodically evaluating business partners' financial conditions, maintenance of licenses and registrations, compliance with laws and regulations, and performance in relation to controls and requirements established under the agreement.

Sixth, Kuiper observed that it is good practice for prepaid-card-issuing banks to use licensed money transmitters for loads and reloads of cards.[29] He noted that licensed money transmitters are subject to examination by state regulatory authorities in each state in which they hold a license, that all consumer funds held by licensed money transmitters must be held in trust, that money transmitters must hold permissible investments equal to or greater than the outstanding obligations, and that additional protections that vary by state can also protect cardholders.

Seventh, Kuiper argued that it is also good practice for card-issuing banks to title accounts and structure programs such that underlying accounts qualify for the maximum amount of deposit insurance coverage possible under FDIC rules.

---

[29] Licensed money transmitters are businesses licensed under state money-transmitter licensing laws. For more information on these laws, see pages 7 and 8 above.

Overall, as Kuiper highlighted, banks can take a number of steps to protect themselves and their customers from the insolvency risk present in the network-branded prepaid-card value chain. Some steps will be taken prior to establishing a relationship with a business partner, such as engaging in due diligence, evaluating a potential business partner's management team, and considering the characteristics of each particular prepaid program. Some steps will be taken as part of the business relationship, such as requiring that accounts be fully funded before cardholders can use cards, building protective provisions into the contract, or overseeing business partners' activities. And sometimes banks can protect themselves simply by following certain practices, such as using only licensed money transmitters for loads and reloads of cards and designing accounts to provide the maximum amount of deposit insurance allowed under FDIC regulations.

C. Regulatory Guidance

Many of the practices discussed by Kuiper are reflected in guidance issued by the Federal Deposit Insurance Corporation in 2008 on how financial institutions can manage risks posed by third parties.[30] In that guidance (in the form of a Financial Institution Letter), the FDIC identifies several risks that can arise from a financial institution's use of an agent or third party (including strategic, reputation, operational, transaction, credit, and compliance risks and other general risks) and outlines a four-part risk management process consisting of (1) forming a risk assessment process, (2) carrying out due diligence related to selecting a particular third party, (3) carefully structuring contracts

[30] Federal Deposit Insurance Corporation, "Third-Party Risk, Guidance for Managing Third-Party Risk," Financial Institution Letter FIL-44-2008 (June 6, 2008).

and periodic review of performance under the contract, and (4) carefully overseeing third parties.[31]

More recently, the Office of the Comptroller of the Currency (OCC), in one of its periodic advisory publications, raised the topic of risks that prepaid card programs pose to financial institutions. In a bulletin published in June 2011, the OCC recommended that those financial institutions it oversees that are active prepaid card issuers and/or program managers should have a comprehensive risk management program to identify, measure, monitor, and control the risks related to these products.[32]

The OCC recommends that such a risk management program should include "clearly defined objectives, expectations, and risk limits for the products offered"; policies and procedures to govern the program; policies and procedures that ensure disclosure to consumers of all pricing, fees, transaction limits, and other requirements or restrictions; robust audit and compliance functions to ensure ongoing compliance; and parameters for reporting to the bank's board of directors whether a program is achieving its stated objective.[33]

In sum, as many segments of the prepaid card market mature and as general-purpose reloadable prepaid cards, in particular, gain acceptance, existing risk mitigation strategies are being reviewed and refined and new strategies are being deployed. In many instances these strategies are similar to ones developed to address banks' more general exposure to third-party risks. However, the nature and complexity of individual prepaid card programs, together with the specific risks posed by particular third parties involved

[31] See Federal Deposit Insurance Corporation (June 6, 2008), pp. 2-9.

[32] Office of the Comptroller of the Currency, "Risk Management Guidance and Sound Practices (regarding Prepaid Access Programs)," OCC Bulletin 2011-27 (June 28, 2011).

[33] See Office of the Comptroller of the Currency (June 28, 2011), p. 2.

in some aspect of program operation or management, merit careful consideration and evaluation by financial institutions.

VI. Conclusion

Prepaid cards, and network-branded prepaid cards in particular, are gaining mainstream acceptance. According to the Federal Reserve's most recent payments study, prepaid card transactions are growing twice as rapidly as payment cards as a whole.

Compared to network-branded debit and credit cards, the value chain for network-branded prepaid cards is more complex. In addition to the usual participants in authorizing, clearing, settling, and processing card transactions, transactions involving network-branded prepaid cards frequently include a program manager, distributor, and a seller.

The presence of these additional service providers implies some additional risk of insolvency along the value chain. And with many more consumers using prepaid cards today, especially bank-issued general-purpose reloadable prepaid cards, more consumers could be exposed to this incremental risk. The recent insolvencies of a well-known prepaid-card-issuing bank and program manager have proven that these risks are real.

However, these events and the many precautions described in this paper demonstrate that there are ways to manage these risks. Moreover, payment networks and banks have both shown that, in the event of insolvency, they can take actions to protect themselves and cardholders from risks posed by their business partners and their business partners' agents. As with any market that is evolving rapidly, risk mitigation strategies

must be reviewed regularly, at the level of both the individual institution and the payment network.