payments system research briefing

August 2005

Federal Reserve Bank of Kansas City

Who's Processing Your Payments?

by Terri Bradford, Payments System Research Specialist, and Stuart E. Weiner, Vice President and Director, Payments System Research

Many people probably assume that banks are the providers and processors of most, if not all, of their payments services. However, nonbanks—defined as service providers that do not accept demand deposits—are also heavily involved in payments activities, providing a variety of services and performing a myriad of roles.

For example, a demand deposit account is established at a bank, but the checks drawn on that account often are produced by a nonbank. When those checks are used at a point of sale, the merchant most often uses check verification services provided by a nonbank to assist in its decision of accepting or declining the payment. Ultimately, when that merchant deposits those checks with its bank, the bank may use the services of a nonbank to process those items. While this is an example of nonbank involvement in the check collection process, it just as easily could have been an example for a debit or credit card transaction or an automated clearinghouse (ACH) payment. The growing presence of nonbanks underscores the operational risks inherent in payments systems. It also raises important questions about oversight and review.

Role and importance of nonbanks

Nonbanks are an important part of the retail payments landscape. They serve as instrument providers, issuing general-purpose, private-label, debit and stored-value cards, money orders, and travelers checks. They provide transaction authorization services as check authorization vendors, fraud system vendors, and certificate authorities. And nonbanks facilitate the processing of transactions as providers of hardware and software and by serving as check outsourcers, card-issuer processors, payroll service providers, ACH outsourcers and operators, and more.

While the presence of nonbanks is significant, it is important to note that the degree of their participation varies across activities and that banks also are involved in many of these activities, sometimes heavily. However, as more payments become electronic, the roles that nonbank participants play appear to be increasing. This enhanced nonbank role, coupled with an increase in use of technology by banks and nonbanks, probably increases the vulnerability of the payments system to various types of risk.

Risks

Many different types of risk can arise in payments systems, and they are often interrelated. Some are broad in scope and affect several parties while others are narrower and affect fewer parties. Of particular interest, as they relate to nonbanks, are operational and system-wide risks, stemming

from such factors as the ever-increasing complexity of technology and networks and the reliance on single networks and software providers.

Operational risk occurs at the firm level. It can be a result of human error, a breakdown in some component of hardware, software, or communication systems, or deficiencies in internal controls. An example is the recent security breach at CardSystems Solutions. Apparent lapses in internal controls and processing procedures resulted in the data for 40 million cards being compromised. While this is just one example, it serves as a vivid illustration that operational risk is not just conceptual. It is reality. In fact, operational risk is thought to be on the rise in light of the heightened dependence of the financial sector, and payments systems in particular, on information technology and communication systems.

System-wide risk is a term coined by the Bank of England, the central bank of the United Kingdom. Not to be confused with systemic risk, which occurs when failure of one party can lead to a large-scale domino effect, system-wide risk is more limited. It is a situation created when disruption to one part of a payments system can lead to a broader disruption. An example of system-wide risk is the January 2003 slammer worm virus, which affected software deployed in many industries, including banking. In this case, Bank of America used affected software and suffered widespread disruption in its ATM services over the course of a weekend. Though these are just two examples, they suggest a higher vulnerability in the payments system resulting from nonbank participation.

Oversight

Such vulnerability raises the question of what public authority has responsibility for supervision of nonbanks. To the extent that nonbanks are providing services to depository institutions, one can look to the Bank Service Company Act of 1963. This act applies to both bank and nonbank affiliated service providers and allows bank supervisors to examine bank-related services provided by nonbanks.

Another question to ask is whether the authority provided under the Bank Service Company Act is still sufficient and/or appropriate, given the revolutionary change in information processing seen over the last few decades. Current supervision of nonbank payments providers is done under the auspices of the Federal Financial Institutions Examination Council (FFIEC). FFIEC supervision is conducted jointly among various federal agencies, including the Office of the Comptroller of Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Association. These agencies develop supervisory standards, examination policies, and examiner training programs.

More specifically, there are currently two examination and monitory programs. One is the Multiregional Data Processing Servicer (MDPS) program and the other is the Regional Data Processing Servicer (RDPS) program. The MDPS is a national program administered by the FFIEC, and there are about 16 nonbank service providers that fall under the supervision of this program. The RDPS is administered by regional and district offices of the FFIEC agencies and encompasses about 110 nonbank service providers.

Both MDPS and RDPS programs use a risk-based approach in selecting, monitoring, and examining service providers, with risk being examined along two dimensions. The first is line of business. This dimension examines the level of risk inherent in various activities and distinguishes among high-risk activities, such as clearing and settling transactions, and average-risk activities, such as ACH processing. The second dimension examines the risk inherent at particular service providers, taking into account the number of clients, number of transactions processed, and so on. As it relates to the CardSystems Solutions' security breach noted above, for example, the FFIEC has begun an investigation to assess security at CardSystems' operational centers, at major credit card companies, and at any banks that may have been affected by the breach.

Whether the growing presence of nonbanks in the payments system requires a significant change to the regulatory structure surrounding payments depends on a number of factors, which are insufficiently documented. Before making specific recommendations, more facts

relevant to questions such as the following would be useful:

1. What is the nature of the operational risk in payments processing? How many incidents are there? How costly have they been, including both costs borne by the payments industry and costs borne by users of the payments services?
2. How often have payments disruptions occurred at vendors that are outside of the current supervision program? How significant are these disruptions?
3. What effect does concentration in the payments processing industry have on risk in payments systems?
4. How successful are institutional arrangements that facilitate the sharing of information on security and operational disruptions to payment systems?

Conclusion

Nonbanks always have been an integral part of the nation's payments system and have shown themselves to be fundamentally important not only in the provision and support of payments instruments, but also in fostering innovation and competition. Given the continued shift from paper-based to electronic payments, it appears that the importance of nonbanks is likely to increase even more in the years ahead. Accompanying this increase will be heightened concerns over risk and new questions about the adequacy of existing oversight programs.

Who's processing your payments? The answer is a host of banks and nonbanks, none of which are immune from potential risks.

This article is based on a presentation by Bradford and Weiner at the NACHA 2005 Payments Conference and draws on the book *Nonbanks in the Payments System*, authored by Bradford, Matt Davies, and Weiner and the working paper *The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview*, authored by Rick Sullivan.

payments system research

Web site: www.kansascityfed.org/home/subwebs.cfm?subweb=9

The Payments System Research Department of the Federal Reserve Bank of Kansas City is responsible for monitoring and analyzing payments system developments. Staff includes:

Terri Bradford
Payments System Research Specialist
Terri.R.Bradford@kc.frb.org
816-881-2001

Fumiko Hayashi
Senior Economist
Fumiko.Hayashi@kc.frb.org
816-881-6851

Zhu Wang
Economist
Zhu.Wang@kc.frb.org
816-881-4742

Nathan Halmrast
Research Associate
Nathan.Halmrast@kc.frb.org
816-881-4721

Rick Sullivan
Senior Economist
Rick.J.Sullivan@kc.frb.org
816-881-2372

Stuart E. Weiner
Vice President and Director
Stuart.E.Weiner@kc.frb.org
816-881-2201