CORE
Metadata, citation and similar papers at core.ac.uk
Provided by UB ScholarWorks

# CHAPTER 10

# FUTURE TRENDS

## Objectives

After reading this chapter you will be able to:

- Review the changes occurring in collections and disbursements
- Appreciate concerns relating to banking relationships and credit rationing
- Understand disaster recovery and contingency planning issues
- Evaluate the trends in treasury organization

## Introduction

Treasurer Bill Fold has been asked to make a presentation to the Board of Directors about the changes he anticipates in the treasury organization. E-commerce and the transition to electronic payments are transforming the fundamental business cycle, and the Board is concerned about treasury's response to this development and to the credit rationing faced by other companies.

Bill wants to focus on core competencies and minimize the operating costs of finance, especially systems investment in areas that are non-core. The Board is anxious to be assured that treasury has anticipated and is prepared to undertake the necessary changes to support these new strategies.

Bill was not caught unawares by the Board's request, particularly in light of the problems of Enron and Arthur Andersen. For a number of months he has been talking to his industry peers and his banks to assess recent trends and their impact . Significant progress has been made at GETDOE in bringing cash management and banking practices to a reasonable level of efficiency.

However, there is concern that the financial services environment is changing so rapidly that current initiatives may be obsolete within a few years. In considering the key developments affecting treasury, Bill, Ann I. Shade, the cash manager and Ric Shaw, the international cash manager, have agreed to systematically compile and disseminate information obtained at conferences, in journals, and through banking contacts and develop a proposed plan of action

As the Greek philosopher Heraclitus noted nearly 2,000 years ago, "Nothing endures but change." In this chapter, we review the likely trend of changes in cash management and banking, and comment on the actions a prudent treasurer might take.

Cash management is evolving as rapidly as any other area of business. Some of the major influencing factors are:

- E-commerce continues to change the business cycle paradigm.
- Consolidation in corporate banking, a trend for over two decades, shows little sign of abating.
- The quest for efficiencies of scale and cost reductions pushes treasury into greater centralization of functions and increased use of electronic methods for collections and disbursements.
- The prevention of fraud, control and risk management issues override all other treasury concerns.

## Trends in Collections

A major cash management trend has been the movement toward use of electronic collections. For the first time in almost a decade the Federal Reserve reported declines in the number of checks processed in 2000 and 2001. As often happens, consumers adopt new trends faster than the commercial world. While the U.S. is still a long way from being a nation that collects and disburses electronically, consumer acceptance of some of the new Internet-based services and digitization of paper formats are helping to accelerate the trend.

### Electronic Bill Presentment and Payment (EBPP)

According to the Harris Poll of April 17, 2002, mobile and Internet technology is used by over 66% of the adult population in the U.S. Although buying products on the Internet and using a credit card to pay is a generally accepted practice, the process of viewing and settling the bill electronically, known as electronic bill presentment and payment (EBPP), is not. Nevertheless, the service has applications for many industries, from financial service providers to telecommunications companies and utilities.

With the emergence of secure e-mail and wireless delivery, it is expected that EBPP use will rise dramatically. The Tower Group estimates that in 2001 almost 50 million consumer bills and over 10 million B2B items will be presented electronically. This number is expected to rise to a total of 2.4 billion items by 2005.

### In the Real World

It should not be assumed that because a payment has been sent through the Internet that the payment will also be made electronically, logical though that may seem. Some banks debit accounts promptly upon receipt of the payment order and then issue payment by check several days later. This allows a bank to use the float for the intervening time. Anyone using an electronic bill payment service should check with their bank to determine how and when the actual payment will be made to avoid late payment and penalties.

Electronic Check Presentment (ECP)

ECP is revolutionizing the collection process by capturing data from a check and converting it into an electronic transmission that is cleared through the banking system. This not only accelerates the presentment of clearing items, but also speeds the notification of any checks being returned due to stop payments or insufficient funds in the account of the payor. In the case of check truncation in the collection process, the paper item often follows the electronic transmission. In point-of-sale situations, the transaction is converted into an ACH item and the check is often returned to the maker for storage or destruction.

Direct Debits

There has been limited, albeit increasing, acceptance of direct debits in the U.S. (A direct debit is where the payor has preauthorized the payee to initiate a debit to the payor's account.) Used most notably by federal and state governments since the mid-1980s to collect corporate taxes, direct debits have more recently been promoted by industries where low-value, regular and frequent payments are due, such as mortgages and insurance premiums. Variable payments, such as phone and utility bills, require that 10 days notice be given to consumers before debiting their accounts. Again, consumers have been faster to adopt this technology than the corporate world.

Tips and Techniques

An emerging opportunity is in using direct debiting for international collections. With much wider acceptance levels in other parts of the world, especially in Europe, some of the larger global banks now offer collection services using local low-value payment systems for direct debits. This avoids the significantly higher cost of wire transfers or availability delays and foreign exchange exposure created by checks.

## Trends in Disbursements

While electronic payments account for only 14% of all payments (see Exhibit 2.4), the advantages of disbursement by paper check are diminishing.

- ECP has made the clearing process more efficient, eroding some of the clearing float benefits of paper disbursements.

- The willingness of trading partners to negotiate "float neutral" terms (where the value date of the electronic payment is the same as when a check would have been debited to the payor's account) is reducing resistance through compensation for foregone mail and clearing float.

- The cost of fraud and of measures to prevent fraud erases many of the pricing advantages of checks.

- B2B e-commerce requires the completion of the transaction by electronic payment.

- Terminal-based ACH is increasingly used for large value, non-urgent payments.

- Payment security over the Internet through such providers as Identrus (www.identrus.com) permits identity and credit verification as well as providing performance and payment guarantees.

- Electronic cross-border, low-value, batch payment options are being developed to expedite global transactions. Some proprietary products are currently offered by global banks to link these payment systems in several countries. Other initiatives such as Step2, developed by the European Bankers Association (EBA), and WATCH, sponsored by NACHA are based on open architecture access.

- The letter of credit process has traditionally been paper intensive and time consuming. The latest developments by companies such as Bolero.net and Trade Card have automated the process and facilitated electronic initiation and completion of the trade. The entire process can now be achieved in days rather than weeks.

Obviously checks are not about to disappear tomorrow. Their value continues as a mechanism to "pay anyone, anywhere". Their future will focus on fraud prevention at all three stages of check disbursement -- pre-issuance, issuance, and reconciliation and retention. Imaging technology has assisted in improving the quality of data capture, the timeliness of transmissions, and access to lists of authorized company signers and quick identification of suspected fraudulent activity. Just -in-time printing has resolved many of the issues associated with the safekeeping and issuance of checks.

## Banking Relationship Concerns

For fifty years commercial lending in America was a buyers' market, with many sellers -- the U.S. banks -- chasing available buyers -- their corporate clients. This happens when an industry is experiencing economic competition and there is too much supply of product for the market to absorb. Sellers often cannot make an adequate return on their investment. Corporations were in charge and banks wined and dined them to sell their wares. Every time a piece of business was put out to bid, a dozen or more banks scrambled to write proposals, cut prices, and promise implementation support, superior customer service, and visits by senior management.

### The New Sellers' Market in Banking

The ending of interstate banking restrictions and the passage of the Gramm-Leach-Bliley Act (1999) allows banks, securities firms, insurers and finance companies the freedom to assign capital to any financial service. And as rational managers, they will seek the greatest

returns for their shareholders. In fact, past strategies were often suboptimal, in that they were made in the context of severe restrictions on their freedom in assigning capital. Banks had to lend money to corporate customers on terms that were not always attractive, because they were restricted to the banking business.

Commercial banks today are in a sellers' market for the financial needs of large corporations. They have the capital to lend or invest and treasurers must go to them, hat in hand, and ask for consideration. Some banks are turning away borrowers, or being extremely selective as to the businesses that they will support, while others are demanding higher prices, more revenue and greater returns. (See, for example, "Who's Getting Hurt by the Loan Drought," *Business Week*, May 20, 2002, pages 122-123.)

Illustrative returns to the bank if a credit line is used or unused are provided in Exhibit 10.1.

EXHIBIT 10.1
Recent Returns on Credit

| | Return on $75 Million Committed Facility | | |
|---|---|---|---|
| Credit Facility | Before Underwriting Expenses | After Underwriting Expenses | With Non-Credit Fee Income |
| Is not used | 6.75% | 3.75% | 13.75% |
| Is used | 9.00% | 8.20% | 10.80% |

Assumptions:

1. The borrower is an "A" rated credit.
2. The credit facility is a 3-year $75 million commitment, $25 million for less than one year and $50 million for 3 years.
3. Risk-adjusted capital ratios (based on the 1993 Basel Agreement on international lending practices) are used in calculating the capital assigned to each portion of the facility.
4. The bank's cost to underwrite the credit is $30,000.
5. The profit from non-credit fee income is $50,000.
6. Simple interest returns are calculated rather than internal rate of return (IRR).

Source: Recent data in the *Gold Sheets* (www.loanpricing.com), a credit reporting and pricing service. Contact Sagner for calculation details

The short-term credit in this situation backs the issuance of commercial paper that is accepted practice in that market as commercial paper is an unsecured instrument. It is obvious that returns are unattractive if credit is the sole piece of business awarded to the bank. The only possibility for the bank to earn its cost of capital is if the credit is not used, if

the underwriting costs are carefully managed, and most important, if there is a substantial profit opportunity from fee income.

Capital Rationing

Banks cannot make an adequate return from credit and must support lending with profits from non-credit activities. This was not recognized in the past due to mediocre bank profitability systems and the high returns from cash management and other non-credit products. These factors have changed in recent years: banks now understand their costs, by product, customer and line of business, and they are seeing dwindling profitability from fee-based business.

There are several factors which compound the problem for companies, including reduced operating cash flow from the global recession and the "9/11" events. Lenders have responded to these developments by supplementing standard contracts with covenants allowing release from funding committed credit lines. Such amendments include "material adverse change" clauses permitting escape if there has been a substantial injurious development in the financial position of the borrower.

Treasurers are facing capital rationing for the first time since the Great Depression. For example, a Fortune 500 company with an AA credit rating was recently forced to accept half of its desired credit line needs at more than double the cost of previous facilities. Furthermore, the participating banks demanded, and received, all non-credit fee business at substantially increased pricing, and banks refusing to provide credit lost all of the other business previously enjoyed.

Where Banks Will Use Their Capital

Alternative uses of bank capital include changing the portfolio of products or investing in U.S. government securities.

- The Product Portfolio. The emphasis on changes in bank product lines will occur as banks focus on more profitable activities, including selected middle market and small business lending and non-credit services, credit cards, trust services, and trade finance. There will be an emphasis on developing less capital-intensive electronic delivery methods, such as the Web-based applications. Bank capital will also pursue opportunities to diversify, emulating the Citigroup (Citicorp/Travelers) merger (1998) that now includes such companies as Salomon Smith Barney and Associates First Capital.

- U.S. Government Securities. The assets of commercial banks are typically about 60% invested in loans and leases, with another 20% in investment-grade securities, 5% in miscellaneous short-term investments, and 15% in non-earning assets. During the decade of the '90s, the amounts invested in U.S. government securities varied from nearly 18% in '93 to 11½% in early 2002 (according to statistics in monthly issues of the *Federal Reserve Bulletin*, Table 1.26). Banks

could decide to invest some of their capital in U.S. government instruments, allowing their balance sheets to return to the safety profile last seen in the early 1990s. (If banks did this, some $375 billion would be removed from lending activity!)

Assume for a moment that a "manageable" amount, say $100 billion, was diverted from normal lending. What is the potential return? Banks lend funds overnight to each other at the Federal funds ("fed funds") rate, which was about 1.80% (in mid-2002). At the same time, 10-year U.S. Treasury bonds were yielding about 5.05%. A completely safe investment would be the purchase of long bonds funded by fed funds borrowing, supported by the capital freed from support for corporate lending as previously discussed. This strategy would result in an annual 3.25% gain (that's $3¼ billion for the banks!) without incurring any underwriting or other expense!

Tips and Techniques

The days of cheap credit are over. Banks have to make enough return on the entire business "partnership" or they will not be interested in the business. A defensive strategy is to:

- Enumerate *all* of the potential business the company has to offer its bankers, and make sure that it's all under the control of the treasury department. In recent years treasurers have been increasingly side-stepped as purchasing and payables departments take responsibility for procurement cards; information technology seizes EDI and e-commerce initiatives; payroll works with banks on direct deposit; human resources controls various benefits programs; and receivables or other business units control securitization. Other financial products that could be included are foreign exchange, derivatives, securities trading, custody, trust and agency services, and the issuance of debt and equity.

- Consider which lenders have the capabilities to provide all or most of the services. Begin discussions with these bankers as to their non-credit revenue requirements for credit business. Consider the relationship history, the competence and interest of the bankers, the breadth of industry experience, and the likelihood that the bank will continue to be interested in providing these services should a merger occur.

- Bid the business in the expectation that the business will be concentrated with no more than one or possibly two banks, effectively excluding all of the others.

Will the Future Bring Systemic Changes?

Throughout the industrial and information ages our financial system has depended on access to credit and the free market has generally done an adequate job in assigning funds to creditworthy users. When subsidies are needed, the government has created

various loan guarantee agencies for specific sectors that need support, *e.g.*, farming, housing, education and small business. These situations involve activities deemed essential to our long-term economic security but which are unable to compete on a "level playing field" with more robust borrowers.

Now that the capital rationing problem has reached the doors of large corporations, it is unlikely that political support would develop for governmental solutions. In the absence of *severe* dislocations, treasurers should not realistically expect a resumption of legislated restrictions on banking.

## Risk Management

The globalization of economic activity requires treasury to actively participate in the management of business risk. Traditional approaches focus on specific risks: insurance for human or property losses; bank credit lines for short-term liquidity problems; compliance officers and lawyers for regulatory concerns; and security specialists, occupational safety and health advisors, environmental engineers and contingency and crisis management planners for a safe and secure work environment.

The treasurer is primarily concerned with financial risk management, driven largely by the volatility of interest rates, foreign exchange, and commodity prices. Specific risk management techniques, including the use of such derivative instruments as forwards, futures, swaps and options, are discussed in chapter 7.

Current techniques include value-at-risk and enterprise risk management.

- *Value-at-risk* (VaR) calculates the risk exposure in a portfolio of financial assets based on historical price patterns. Various proprietary models attempt to measure risk covariance to a selected degree of statistical confidence. VaR focuses on lines of business that involve high risk or investment yet result in low returns. There are two significant problems in using VaR:

    - Risks for which pricing is not available and may not be adequately considered, i.e., the political risk of a coup d'état or currency devaluation in a foreign country, such as the 2002 situation in Argentina when the country defaulted on its international loans and faced credit and political crises.

    - The "perfect storm" problem, when risks that normally are offsetting are concurrently adverse. A recent example is the collapse of Long-Term Capital Management (in 1998), when illiquid markets and political tensions caused the prices of U.S. Treasury securities to exceed historical trends.

- *Enterprise risk management* (ERM) attempts to integrate multi-source risks in a comprehensive organizational strategy. This approach considers risk as ubiquitous, requiring the coordination of all relevant business and political

situations. For example, the Ford-Bridgestone-Firestone tire recall (in 2000) would normally escape traditional risk management oversight, but would be captured in a comprehensive ERM program that evaluates potential business risks. ERM analysis includes the risk of a significant product defect by assigning probabilities and worst-case scenario assumptions to specific situations that could significantly impact a company.

In the Real World

One consumer products company (Hallmark Cards, Inc.) that uses ERM has implemented a multi-step process: identification of the risk, measurement, formulation of a cost-effective containment strategy, implementation of tactics to effectuate the strategy, and continuous monitoring. The company is supported by the services and technology of a major insurance broker, Marsh & McLennan.

## Control and the Management of Disasters

The problem of control is present in all treasury functions, and may be of greater concern today than in previous eras. This is due to several reasons:

- Staff downsizing, which compromises the separation of accounting and financial duties.

- Technology advances, with an accompanying explosion in the exchange of data through interfaces supported by computers, telecommunications and the Internet.

- A general crisis in corporate governance, as employees, stockholders and customers watch trusted institutions fail to protect the integrity of the financial system.

- The failure of business to assign responsibility for protecting the most important “new” economy resource -- not cash or any physical asset -- but intellectual capital.

### Employees

Employees represent a significant treasury threat as they are inside the organization, know the security measures utilized in most areas (or lack of security), and may be difficult to detect in any wrongdoing. They may be hostile for various reasons, such as a perception of "injustices" against themselves or their colleagues, the desire for financial gain, “the challenge”, or simply boredom. Bank products discussed throughout this book work well when properly administered, but may be circumvented by a determined individual and/or collusion.

Defenses against adverse employee actions include the following:

- Hire responsible, trustworthy employees, including clerical workers who may be selected or transferred to treasury with minimal background checking. It is the office staff with access to treasury information systems that can commit theft or fraud. Bonding of employees in positions with significant fiscal responsibility is an increasing trend.

- Monitor employees who are in sensitive positions for changes in behavior or attitude due to financial problems, family strain, addictions or psychological illnesses, or other stresses. The format can be simple observation (e.g., conspicuous spending, personal telephone calls, workplace absences, changes in physical appearance) to more structured programs, such as mandatory personal financial statements and periodic medical exams.

- Although it may be distasteful, consider electronic surveillance of telephone calls and e-mail messages. There is a diversity of court findings on whether employees can be subject to such scrutiny as the law is still developing on privacy rights, although increasingly courts are ruling in favor of companies being allowed to monitor employee use of company-owned computers.

Electronic Devices and Barriers

A breach of security can occur at various points: accessing hardware or software, in telecommunications lines, and at banks or other vendors. Merely enclosing a facility and using guards or watchdogs does not adequately safeguard technology. Security must begin with entry restrictions to areas using electronic devices and barriers. Access to treasury information systems involves identification of the user with a password, a special badge or key, or a scan of the eye or fingerprint.

The exchange of data between bank and company computers may involve multiple telecommunications connections. The resulting exposure from these possible points of intrusion has resulted in numerous occurrences of eavesdropping and theft. All communications should pass a firewall barrier to protect internal traffic from outsiders (or internal systems from each other), with all messages examined and entry barred if predetermined criteria are not met. In addition, telecommunications cables should be encased in steel or pressure-sensitive conduits, which signal when there has been an intrusion on the line.

Computer and telecommunications systems can be protected by scanning programs to detect intrusions by:

- Computer virus infections. Viruses can be monitored by observing:

    - Processing time slowdowns
    - Programs trying to write to write-protected media
    - Unexplained computer memory decreases

    - Files that cannot be located
    - Unusual computer messages
    - Differences in length between active and archival files

- Use of unauthorized passwords or repeated password attempts

- Efforts to enter systems for which the user is not authorized

- Log-ons at an unusual time of day or on weekends

- Significant deviations in patterns of usage

Anti-virus programs should be enabled to run automatically at regular intervals. The most recent versions of this type of software run all the time in the background.

Disaster Recovery

Prior to the events of "9/11", disaster recovery concerns focused on whether banks had a dedicated disaster recovery or contingency planning manager; a comprehensive plan listing precise steps in the event of a disaster; adequate technology support; automatic hardware, software and telecommunications switching; and power backup including dual power feeds and auxiliary power systems. Although those actions are still relevant, other considerations should be included in catastrophe planning, including actions by both the bank and the company.

- Prevention. Do the bank and the company have adequate physical security, including detection and protection systems? Are there established procedures for control and access? Is regular data back-up required for all systems and data files, and are the media archived to a secure offsite location?

- Evaluation and mobilization. Who are the company and bank managers in a disaster recovery incident? Is there a specific plan for critical functions, such as hardware, software, technical support and communications? What expectations are there for resumption of processing and restoration of the primary site? Is there a regular testing program of established procedures? Has the bank experienced an actual disaster? If so, what was the result? What steps has it taken to remedy any deficiencies in the plan?

- Backup site recovery. Are the backup sites sufficiently distant as to be unaffected by the disaster? Have arrangements been made with a third-party disaster recovery vendor, such as Comdisco or IBM?

Your bank will not share specific plans and procedures with its corporate customers. However, you should feel satisfied that the bank and your company is totally prepared for just about any attack or natural calamity that may occur.

In the Real World

Following “9/11”, many companies that were not directly effected by the disaster generously offered their crippled competitors floor space and equipment pending their ability to reestablish independent facilities. Although these accommodations had not been agreed to by formal arrangement, they were successful due to the similarities of the business and/or the technological platforms. This has led to an increasing number of companies establishing mutual back-up sites with traditional but geographically remote competitors, providing an alternative solution to a more costly, redundant back-up facilities.

Computer Security

Despite the planning for disaster, the “9/11” attacks disrupted typical corporate life for weeks, impacting nearly everyone who had to be in daily contact with their bankers. Most affected treasury managers were able to function using a back-up site or other facility.

Often a second site is a laptop computer, which can provide access to bank account data and other information from home or any location with telephone service. Many New York and Washington treasurers reported that they grabbed their laptops and relocated, often to their homes or to company offices in safer locations. However, this convenience could potentially be a “land mine” for the unsuspecting, because there is a large potential loss -- the data that resides on a laptop which could be worth millions of dollars to a smart thief.

Tips and Techniques

Here are some ideas to consider in protecting your computer and the valuable information it contains, such as bank account numbers, key company contacts, account balances, investments, pending debt or equity deals, or other financial matters.

- Conceal laptops. Any observant thief can spot a laptop; the shape of the briefcase is distinctive. Put the computer in a bag that doesn’t look anything like computer luggage, such as a gym bag – no-one wants to steal used gym equipment.

- Hide passwords and codes. Don’t put secret access information on a post-it note on the computer, on the hard drive, or anywhere in the carrying case. Memorize it, or, if that’s not convenient, keep it in a wallet but label as the mother-in-law’s phone number.

- Encrypt files. Several programs are commercially available to encrypt data, rendering files unreadable to anyone without a “key”. The latest versions sell for about $50, and are well worth the expense when working with files that contain sensitive information.

- Keep the computer in sight at all times. Bags are often left unattended in airports and hotels while the owner is off to buy a newspaper or on the phone, and two seconds is all it takes for the bag to disappear. When going through airport security put the laptop through last and do not let it move into the x-ray machine until you're allowed to pass through the detector. If you are stopped for an additional security check, make sure the computer is in your line of vision at all times.

- Securely lock the computer. If you are forced to go to an emergency site (other than home), tether the computer to immovable furniture with a steel cable lock that fits in a slot in the machine. New colleagues at the site may be absolutely trustworthy, but an intruder can grab a laptop and disappear in the time it takes to go to the bathroom or get a sandwich.

- Back-up data, frequently. Many financial managers do not regularly backup data to alternate media, such as the main server or an external floppy or CD-ROM drive. This should be done before the computer is shut down — *every time* that new data is entered. Store the back-up copy in a separate location, otherwise, the thief could take the data, the computer and the second copy. In an emergency, or while on the road, send copies of changed or new documents in an e-mail to the office.

- Load applications only. If possible, keep data on a central remote server on the Web and have only the applications that allow the retrieval of the information loaded onto the laptop.

- Keep vital contact information with the computer. If a disaster has occurred and working from the laptop is the contingency plan this will be effective, only if there is also a record of all the necessary phone numbers and codes, including the numbers for the banks and their emergency sites. Keep a detailed list of everything that may be needed in the computer bag.

- Let the banks know the company's plans. Banks have devised various security and access codes to protect the company's assets, and they need to be fully informed of your emergency arrangements, alternative phone numbers, and other disaster recovery plans. They may require proof of identity before executing any significant transactions, such as wire transfers, particularly if the communications are routed to an alternative bank site. File contingency plans with them and review them every six months. Also, don't wait for a disaster to occur to test the plans for the first time. Arrange with the bank to test the smooth functioning of the plan.

## Organization Of The Treasury Function

Technology is the driving force and enabler behind many of the changes in treasury . It is the timely availability of information that allows balance management to be consolidated, liquidity to be optimized, and global risks to be measured and monitored. This section discusses the role of technology in enabling some of the major trends in the organization of the treasury function:

### Centralization through Shared Service Centers (SSCs)

When business units perform the same function throughout a company, such as payroll, there is an opportunity to eliminate the duplication by using an SSC. Often described as "insourcing", an SSC acts as an independent business bureau within the company to present a single interface with the internal and outside worlds. Companies have been using SSCs for legal staff, real estate management, advertising, and travel services, for many years. Applications in treasury, accounts payable, and accounts receivable are more recent. In larger companies the SSC may evolve to be the in-house bank for the internal entities of the company, undertaking all the foreign exchange and currency management.

There are several critical elements to developing a successful SSC:

- Efficient communications and technology infrastructure to provide common platforms, often involving enterprise resource planning (ERP) systems.

- Responsiveness to the needs of business units, often attained through SLAs to assure an acceptable level of performance.

- An organizational commitment to centralization.

The launch of the EMU and the euro (see Chapter 7) has been a major driver in companies' establishing SSCs for treasury functions to help them compete more effectively in the new regionalized global economy.

### Enterprise Resource Planning (ERP)

ERP systems claim to offer a common technology platform throughout the company, between and across the business units. A key technology issue for treasurers has always been integration with underlying business systems to obtain risk and exposure information for senior management reports. In theory, enterprise-wide systems offer end-to-end business processing, from data input at the raw data level of accounts payable and receivable through inventory management, order processing, working capital management and currency forecasting. Major providers of ERP systems are SAP, Oracle, J.D. Edwards, SunGard and PeopleSoft.

In reality, implementation of an ERP system is time-consuming, painful and expensive. Companies often compromise the integrity of the concept by using one system for some functions and others for such specialized areas as treasury, or by having different versions of the software on different platforms. Both situations force further internal integration of systems. In addition, another key technology issue is that ERP systems require an interface to external sources such as electronic banking and market information systems. While banks are increasingly trying to provide "plug-and-play" interfaces with the major systems used by their clients, the evolving nature of the technology makes full compatibility difficult. ERP systems are likely to remain a viable tool for only the largest companies.

Outsourcing

Once a function has been centralized, the treasurer is in a position to determine whether there is an opportunity to outsource non-core functions. The decision has been made easier due to the proliferation of application service providers (ASPs) and business service providers (BSPs) offering Internet-based applications and services. ASPs allow a company to outsource particular applications, such as netting and treasury workstation routines. BPSs will undertake entire functions, such as the back-office processing of a cash management operation.

The justification for outsourcing is that a specialized third-party provider can perform the function more cost effectively, and with greater expertise and specialized technology investment than the company. Some of the benefits that can be expected are reduced exposure to technology shifts and market changes, reduced overhead and operating costs, and the freeing of internal resources and technology dollars for investment in core businesses. Outsourcing provides a turnkey solution, and the expectation that the partner will retain a high level of expertise and leading edge solutions. The major concerns with outsourcing are the relinquishing of control and information to an outside party, and a potential loss of flexibility by being tied to the partner's technology.

Open Architecture Electronic Banking (EB)

Companies are increasingly intolerant of proprietary formats and expensively integrated systems that tie them to a single bank 's system. Several bank-neutral platforms, such as GEIS and BankLink have been introduced offering the flexibility of standardized interfaces with multiple bank EB platforms. This allows companies to change or add banks when necessary, without losing integrated interfaces. In Germany, the banks cooperated in developing a single EB platform called Multicash.

## Future Role Of The Treasurer

Over the last decade, the role of the treasurer has been elevated to the rank of strategic partner and a key participant in the senior management team. With certain operational tasks removed or outsourced, the treasurer is now an advisor to the board on business

strategy and global risk and liquidity management, and is, effectively, a "virtual treasurer": Exhibit 10.2 illustrates the evolution of the treasury function.

[Insert Exhibit 10.2 here]

Even though banking relationships are consolidated and bankers are assured of profitability, treasurers will have to pursue credit alternatives to traditional lending: trade credit arrangements, seller financing and receivables factoring. Aggressive management of the working capital can minimize the cash conversion cycle, the number of days in the operating cycle less the payment period for expense factors.

Collection and disbursement activities should be rigorously scrutinized, as should the need to finance inventory through the implementation of just-in-time (JIT) procedures. Treasury must become the company consultant on cash and financial issues to reduce dependence on credit facilities. In summary, treasurers will have to work harder and smarter, making certain that their banks receive adequate compensation and that their company's operations are efficient and cost effective.

## Summary

The inevitability of financial change requires treasurers to be cognizant of new products, new regulations, and new opportunities to assist their organizations. Traditional U.S. cash management practice will become more electronic, and Internet-based technologies will drive the integration of accounting, treasury, sales, purchasing, and manufacturing systems. Bankers will use their scarce capital for profitable business opportunities, and will reduce their lending exposure while increasing pricing. This will force companies to call upon the skills of finance to be smarter in managing the working capital cycle. At the same time, risk management and security concerns have become critical considerations in managing company resources. The challenges and opportunities of the 21st century are indeed significant!

Bill and his staff are convinced that there are many economies of scale to be realized by centralizing certain functions in the cash management area. Some of the projects they are considering include:

- A shared service center, building off the SSC that already exists for other functions in the company.
- ASPs, which can provide an attractive alternative to developing in-house capabilities.
- An intracompany netting system.

They do not think the company is ready for further outsourcing, as there is still considerable work to be done on centralizing and then determining the core competencies. Bill is not sure that he is comfortable with having a third-party provide the interface in handling customer inquiries. In preparing for his meeting with the Board of Directors, Bill realizes that there is work to be done to prepare treasury for the future.