Microbanker BANKING TECHNOLOGY STRATEGIES

January 1, 2002
Volume 3, Number 1

www.microbanker.com

Fearless Predictions For 2002

By Roy W. Urrico

What will be the lingering impact of the September 11th attacks? Is the recession in retreat or is it just beginning? How will banking technology be affected? These are questions surely for better minds than this humble writer but there is a tradition at Microbanker that needs to be maintained. So I offer my best assessment of the industry with the hope that the year 2002 will be a better year for the health, stability, and recuperation of the world as a whole — and that the financial technology industry will play a major role in that recovery.

"Security and risk management (from safety and economic perspectives) have emerged as the two critical 2002 issues for this industry."

The economic consequences of the 9-11 destruction of the World Trade Center cannot be underestimated, particularly in the financial services industry. The figures — compiled by Computer Science Corp. (CSC) in the *14th Annual Survey Of IS Management Issues* — are staggering:

- TowerGroup guesstimates a $3.2 billion price tag for securities firms to replace the technology shattered in the World Trade Center and neighboring buildings.
- Computer Economics projects it will take $15.8 billion to repair IT and communications capabilities in New York City and Washington DC.
- American Banker reports analysts' estimates of potential property and casualty insurance losses ranging from $30-40 billion.
- Best's Review predicts that workers' compensation costs could reach $6 billion.
- Anticipated life insurance losses are placed at $3-5 billion. Reinsurers' loss projections "would be equivalent to their worst-ever catastrophe payouts."

Those are the dollar amounts; the effect on the corporate psyche is another story. Coupling that business demeanor with an ongoing economic retraction does not make for a promising 2002 for financial technology.

Security and risk management (from safety and economic perspectives) have emerged as the two critical 2002 issues for this industry. "Risk management almost always resumes a strategic profile in times of economic uncertainty or recession. A variety of risk dimensions are relevant to this initiative, including fraud, dynamically defining customer profiles for credit products, and analyzing and managing portfolio (product, geography, customer segment) risk levels," Meridien Research, a financial industry technology analyst firm, says in its *Top 10 Strategic IT Initiatives in Retail Financial Services for 2002.*

IN THIS ISSUE

Even though the Federal Deposit Insurance Corporation in a report forecasts, "FDIC-insured institutions remain in generally strong financial shape and will continue to provide credit to finance economic recovery," they also warn that banks are likely to face significantly more difficult economic conditions in the months ahead.

That being said there are some areas to look at for technological activity.

Security, Long A Necessary Issue, Becomes A Vital IT Function

The thought process involving security, i.e. identity theft, fraud, privacy, has changed dramatically from a necessary function to a vital risk management process. The September 11 terrorist attacks have forced North American businesses to radically reassess their ability to resist a security threat.

Prior to Sept. 11th, according to Kroll, Inc., a risk-consulting firm, information protection and employee integrity were the top security priorities. Now executives are concerned with emergency preparation, business resumption planning, and physical security as their leading issues.

"The thought process involving security, i.e. identity theft, fraud, privacy, has changed dramatically from a necessary function to a vital risk management process."

Among Kroll's findings:

- Only 43% of respondents gave themselves a positive rating on their organization's ability to manage security risks' prior to 9-11. But 89% expected that to change within six months.
- Preceding 9-11, only 34% said emergency planning was important. That number has jumped to 86%.
- Prior to 9-11, only 38% cited business resumption planning as important. That figure is now 80%.
- Only 40% identified physical security as a priority prior to 9-11. Now 89% have placed it at the top of their agendas.

What does this mean for the financial services industry? In its survey taken before September 11th, CSC identified "protecting and securing information systems" as the most often mentioned issues from financial services industry respondents. "The most likely outcome [following the attack] will be even more reliance on IS to manage risks, improve efficiency and provide flexibility and resilience in the face of unknown threats and difficult economic times," states Jim Cook, president of CSC, in his company's survey.

What are the major concerns? The Ernst &Young's Center of Competence for Private Banking in conjunction with the Ernst &Young Fraud Investigation Group produced a survey on private banking. Among their key findings:

- Respondents identified fraud as a key operational risk, both in terms of profitability and reputation. (Some banks have lost up to $200 million from detected frauds.)
- They identified the key fraud areas as account transfers, signature falsification, and misleading pricing of securities.

CSC's new updated poll taken in late September 2001, shows that information security has become the main concern for North American IS executives, and the *number one* issue for financial services executives around the world.

In order to stay competitive institutions have created enterprise infrastructures with multiple internal and external entry points. That has made those systems more susceptible to invasion. These include data warehouses, network storage systems, and even desktops or, in other

Banking Technology Strategies is published twice a month by Microbanker Inc., P.O. Box 708, Lake George, NY 12845. 518/745-7071 Fax 518/745-7009 E-mail: royurrico@microbanker.com. Price: $395 US and Canada; $435 foreign.

words, customer support applications, finance/accounting/administrative/HR systems, and sales and marketing applications.

"These are business functions, not IS technological functions," says Joseph Stafford, vice president of CSC's Global Information Security Services. "The data indicates that executives are beginning to acknowledge the role of information security as a business issue rather than purely a technological implementation issue. Consequently, the value of information security is being introduced to the boardroom in a more visible and compelling manner."

This is supported by a recent Star Systems report that reveals almost 50% of all Web shoppers would open there wallets wider if better security technologies were in place.

The most notorious of fraud transgressions is identity theft and should receive the majority of attention from the financial institutions in the near future.

"The most notorious of fraud transgressions is identity theft and should receive the majority of attention from the financial institutions in the near future."

Identity theft, according to industry sources, affects as many as 750,000 new victims each year and costs consumers, merchants and the financial industry billions of dollars. Identify theft is when personal information is stolen — many times from Web sites or by eavesdropping on cell phone conversations while consumers make purchases.

The Federal Trade Commission reports that its fraud hotline receives about 1,700 calls each week. The Treasury Department's Financial Crimes Network reports that identity theft documented by financial institutions nearly tripled between 1999 and 2000. The Social Security Administration says reports of misuse of Social Security numbers on its fraud hotline increased by more than 500% between 1997 and 2000.

Reported occurrences of identity theft are expected to more than triple — from 500,000 in 2000 to 1.7 million in 2005 — and the financial institutions' tab will swell 30% every year — to more than $8 billion in 2005, according to a report by Celent Communications.

However identity theft and outside forces are not the only threats to security. Those implementing or planning on implementing security policies and systems are mainly focused on network intrusion, virus attacks, and server host protection, or as CSC calls it, the so-called "outsider" threats.

In 2002, maybe financial institutions, particularly in the U.S. and Canada, will turn their attention to the most damaging security threat, the "insider" problem, e.g., employee malpractice, data theft, and electronic fraud. These, says CSC, "are acknowledged in recent FBI and Computer Security Institute (CSI) surveys as the larger and potentially more damaging security threat." Some studies place the total percentage of fraudulent incidents in U.S. committed by insiders at 66%.

Internal fraud is a subject that most North American institutions prefer not to publicize but they will need to address sooner, rather than later. According to Ernst & Young's Private Banking survey:

- Relationship managers, mostly acting alone, committed the majority of frauds over the last five years.
- Nearly 80% of respondents are concerned that a significant fraud could occur within their organization.
- 67.5% of all identified frauds were committed by employees, almost a third of which were by management. Nearly half had been with the firm for more than five years and over a quarter for more than 10 years.

"Internal and external security concerns have been elevated to high levels at business units. Institutions face loss of trust with customers and the ever-present eyes of regulators if security breaches occur in either domain," warns Meridien.

Many Happy Returns On Investment

The industry has issues with security of information, electronically connecting to customers, suppliers and partners, aligning information services with corporate goals, and improving or replacing systems applications, enterprise-wide services and business efficiency.

However issues will not necessarily dictate the forthcoming IT projects. After security the most significant technology focus areas will be on risk management and return on investment (ROI). This, of course, is not the sole perspective of the banking industry as most business sectors are involved in cost-containment and survival tactics due to the economic slowdown.

Though many financial services firms admit the need to update obsolete systems is a priority, rarely are they choosing replacement strategies, explains CSC. "More common are projects to improve a function or process, and projects that implement an enterprise-wide solution."

Overall, retail financial services organizations worldwide are projected to expend $33.8 billion in 2002 on strategic technology initiatives, according to Meridien Research in its *Top 10 Strategic IT Initiatives in Retail Financial Services for 2002*. That is down 6% from the $36 billion 2001 estimate.

"Clearly, the year 2001 contained some surprises for the financial industry, including the rapid economic bust for scores of dotcom vendors, the arrival of a global economic slowdown marked by regional recessions, and the tragedy of an unimaginable terrorist attack. In the wake of these developments, financial institutions generally closed the vault door on new IT spending initiatives across the board," says Bill Bradway, Meridien's cofounder and research director.

However, there is another mindset taking place as well: "To avert a year 2000 calamity, and then to capture the power of the Internet — bankers now are cutting back on technology investments, trying to get the most out of the money they have already spent," says David Blanton, executive vice president of banking solutions at Computer Sciences Corp. "...Faced with a slowing economy and the increasing chaos of the Internet marketplace, bankers...are focusing more on finding ways to get more out of the investment they have already made."

"Whether called service bureaus, third-party providers, or application service providers (ASP), there is no doubt that outsourcing IT has become an established viable alternative to on-site development..."

Return on IT is also listed by Meridien as the top 2002 IT initiative. Meridien defines return on investment as "A differentiating measure of success for lines of business and IT, ROI analysis is based on metrics — the ability to measure with recurring precision and consistency. Frameworks with relevant, achievable business targets measured against staffing, IT, and marketing resources become the culture," states Meridien.

Gaining A New ASP-ect To Financial Technology

Whether called service bureaus, third-party providers, or application service providers (ASP), there is no doubt that outsourcing IT has become an established viable alternative to on-site development, and that it is growing in popularity among financial institutions of all sizes.

System development in areas that include customer service, back office, sales and marketing, administration, knowledge management, procurement, data warehousing and R&D are being outsourced, at least in part, by more than 70% of financial service companies surveyed by Computer Science Corp. (CSC) in their *14th Annual Survey Of IS Management Issues*.

"Forty-four percent of banks use software packages from third-party providers, but they extensively modify them — an expensive proposition," says Jackie VanErp, vice president of third-party relations in CSC's financial services group. "And 91% are outsourcing some aspect of their information-technology operation."

Development, Web hosting, network systems, desktop distributed help desk systems and data centers are the five most outsourced activities, according to CSC. In the future we are likely to see more of the same activities as well as application hosting being outsourced.

Why the great interest in ASP implementation? *The Financial Impact Of ASPs*, a study conducted by IDC, discloses the high ROI and payback for ASP clients. Among the other key findings:

- ASP implementation generated an average five-year ROI of 404% and almost half of the organizations in the study received payback within six months.
- Forty-four percent of respondents experienced an ROI greater than 100 %, while 12% report ROI returns of more than 1000%.
- The average payback for an ASP outsourced solution was 1.33 years on an average total investment of $4.2 million. The average initial investment was $399,000.

Checks Are Decreasing, Barely, While Electronic Payments Are Increasing

The results of the Federal Reserve System study of the U.S. retail payments systems are rather interesting, if not outright astounding in some cases. Approximately 1,300 financial institutions, including banks, thrifts and credit unions, and 89 electronic payment processors responded to the surveys, the first comprehensive studies of the retail payments market by the Fed since 1979.

Among the more significant findings is that there is "a strong migration toward electronic payments, with paper checks occupying a smaller share of the payments market compared with 20 years ago."

Even though checks may be occupying a smaller share, it does not mean they are going away anytime soon. In fact since 1979 there has been an increase in the number of

checks written from 32 billion to almost 50 billion. Add to this another 30 billion retail payments (or 40 percent of all noncash payments) made annually by electronic means, such as credit cards, debit cards and the Automated Clearing House (ACH).

The study results also show that checks have declined from about 85% of noncash payments since 1979 (when the last study was done) to approximately 60% today. However that is 60% of 80 billion noncash payments (compared to 85% of 37 billion in 1979).

The so-called paperless society has put an enormous strain on payment processing and will continue to do so.

Not Bricks, Not Clicks, Its ATM Flicks That Head To Number One On The Customer Usage Charts

Now is a great time for financial institutions to cash in on expanded ATM uses. By 2003, IDC predicts that ATMs will surpass the branch as the highest volume U.S. banking channel, with over 13 billion annual transactions. The availability of Web-enabled ATMs gives banks the opportunity to "cross-pollinate" online banking and ATM services, which IDC says "can have significant implications on banking products, customer relationship management, and customer acquisition strategies. IDC also believes the timing is right in "the context of a larger multichannel delivery strategy."

"Now is a great time for financial institutions to cash in on expanded ATM uses."

Nevertheless, as transactions, and the quantity of ATMs grow, IDC thinks banks will encounter gradually more complicated issues, including increasing ATM support costs, identifying new revenue streams, and potential new accessibility regulations under the Americans with Disabilities Act.

The machines have become so ubiquitous — and Americans so comfortable with them — that there is great opportunity to offer a range of new services, according to an annual survey of consumer attitudes released by Star Systems, the electronic payments network.

Customers want expanded banking services such as balance inquiries and the ability to make deposits at "foreign" ATMs (those not operated by a cardholder's financial institution). In addition, a number of customers want to purchase postage stamps, obtain sports and theater tickets, and pay bills at their ATMs.

Consumers were asked which ATM-based services they would consider "extremely appealing." Their responses included:

- 37% — conduct balance inquiries.
- 31% — make transfers among accounts and obtain statements.
- 29% —make deposits.
- 28% — buy postage stamps.
- 23% (each) — pay bills; buy event tickets.

EBPP: It's Getting There

Electronic bill presentment and payment continues a slow, steady climb.

Fifty-five percent (55%) of online bill paying consumers chose their bank as their preferred central site, while just over 10% chose their Internet service provider or a private site, according to a Yankee Group survey.

The survey notes that the developments of e-commerce strategies by communications providers, utilities, credit cards, Web portals, provide consumers and businesses with a wide variety of options for the electronic delivery of their bills and invoices. In addition using marketing and incentive programs, billers are slowly driving more of their customers to the Web to receive and pay their recurring bills, but the transactional nature of electronic bill presentment and payment (EBPP) presents an outstanding opportunity for financial institutions to play the leading role.

"Banks, which in the past used a 'wait-and-see' approach to EBPP technology investment, still have a distinct advantage thanks to the churn-resistant nature of their customer base, and the increased acceptance of online banking among high-end customers," explains Paul Hughes, director of Billing & Payment Application Strategies at the Yankee Group. The next step, he says, in continuing to build adoption is to improve bill distribution via a standards-based delivery channel, and ensure that the end customer can gain access to as many bills as possible, thus demonstrating the true value of what EBPP is trying to provide."

There are other positive signs for the electronic payment advocates, if they are patient.

- Nearly three quarters of companies believe "critical mass" in electronic bill payment and presentment (EBPP) won't happen before 2004, according to

Forrester Research. The problem right now is that comparatively few banks now offer bill presentment online and few billers make bills available. A "consumer hub" that offers a single "switch" for bills, payments and money transfers between financial institutions will break the deadlock. Forrester also predicts that by 2006 consumer demand for EBPP will triple.

- As Internet usage swells so does electronic bill payment frequency. That is a finding of a 2001 research study by SYNERGISTICS RESEARCH CORP. The number of electronic bill payment users, according to SYNERGISTICS, is currently reported to be 25% of Internet users, a big jump from below 10% in 1999. Not surprisingly, usage shows a wider acceptance among younger consumers. One-third of those aged 18-34 are current users of electronic bill payment, compared with one in six of those age 65 or older. Usage is also higher among those in the $100K+ earnings category, with one-third of that group using EBPP, while less than a fifth showing usage from the under $25K range.

"There are many indications the account aggregation on a single financial services Web site is ready for prime time."

The results of a new nationwide survey by Boston-based strategy firm Dove Consulting confirm that since 9-11, seven percent of U.S. consumers have either signed up for online billing or increased the number of bills they are now receiving online-based on concerns over handling mail and late bill payment. Another 32% of respondents to the survey said they have started thinking differently about receiving statements online in the weeks following the Anthrax scares.

Aggregation Emerges From Bleeding Edge

There are many indications that account aggregation on a single financial services Web site is ready for prime time.

According to the Yankee Group's annual *Technologically Advanced Family Survey*, which measures consumers' experiences and interaction with more than 100 products and services, most online bill paying consumers want their bank to take a leading role in the aggregation of their recurring bills.

In a recent Jupiter Media Metrix Consumer Survey 45% of U.S. online financial consumers report having no major concerns about consolidating their accounts at a single institution. According to Jupiter analysts, consumers will combine their accounts with one institution as diverse financial offerings — such as banking, lending, brokerage and insurance — continue to integrate and mature.

According to the survey, the small quantity of online financial customers who have trepidations about account consolidation mainly mention institutional instability (18%), excessive sales solicitation (11%) and the effort required to shift accounts (11%). However, says Jupiter, those concerns will ultimately diminish, thus clearing the path to faster consolidation (among financial service providers) and convergence.

Closely aligned with the growth of account aggregation is the emerging portal solutions, which Meridien rates as one of the top IT initiatives for 2002. "Account aggregation's value is a foundation, enabling customer-level value propositions around wealth management business strategies, self-service analytical solutions, and financial portals that serve customers and employees."

Not Even Concerns Over Security Can Help Smart Cards In The U.S.

The joke in the chip-based card industry has been that when asked "when will smart cards have that breakout year in the U.S.?" the answer would invariably be "in two years." That has been a rolling two years since the mid-80s.

Well it seems that those two years are about to expire. Given all the concerns over security, privacy and fraud, smart cards need to emerge in 2002 or face the fact that it is never going to happen here in North America. Smart cards have faced, and will continue to face an uphill battle because of two major issues — consumer demand and economics.

First, there has been no substantial consumer drive to utilize a chip-based card despite the marketing efforts of companies like American Express and Visa. (Amex issued about eight million Blue cards; and Visa is expected to issue about seven million chip-based cards through alliances with Fleet and Target).

Secondly, while smart cards use would certainly be a boon to banks and merchants that now shoulder the burden of fraudulent credit and ATM card usage, the price tag of the cure may be more than the cost of the malady.

Chip-based cards cannot be duplicated, therefore they cannot be skimmed, unlike magnetic-swipe cards. Skimming is when credit cards or ATM cards with magnetic-stripes are swiped through devices ("skimmers") that capture information contained on the mag-stripe at

bogus ATM and POS machines (some are equipped with small cameras). Unscrupulous waiters and waitresses at restaurants also use skimmers to capture mag-stripe data. The skimmers are used to steal the name, credit card, and PIN numbers of unsuspecting consumers. With that information, duplication of cards is made possible.

Skimming already represents a large percentage of scams and is considered the fasted growing area of fraud involving magnetic-stripe cards.

According to the New York Daily News, skimmers are believed to have been behind the theft of thousands of dollars in November alone from accounts of Citibank and Chase customers on Manhattans Upper Eastside.

However, fraud in the U.S. is not as big a problem as it is elsewhere, points out George E. Devitt, Hypercom svp/cmo. He also cites the cost of converting the billion or so magnetic cards currently in use in the U.S. to smart cards. The upfront tally outlay could run as high as $2 billion. Then there is the continuing cost of replacing those cards every few years.

"Smart cards may have a play in e-commerce but you will see a combination of magnetic stripe cards with biometrics, which could go a long way to eradicate fraud," says George. "We will probably never see the acceptance of smart cards in the U.S. because fraud is a relatively small problem in the U.S.," compared to Europe and other countries where "fraud was rampant."

The news is not all bad for smart cards. There has been progress. Smart card usage in the United States and Canada rose 37% in 2000 from 1999, according to a report from the Smart Card Alliance.

The total number of smart cards manufactured for use within the United States and Canada for 1999 was 20,775,000. In 2000, the research shows that number grew to 28,430,000 — a 37% growth.

That is not enough suggests Celent's latest report, *Smart Cards in U.S. Banking: Is the Chip Hip?* Smart cards have not only failed to find a valuable application to support in the U.S. market, says Celent, but companies that are touting them as fun and trendy in order to lure converts will not succeed either.

Celent suggests that while there is renewed U.S. interest in smart cards, a strong mandate for their use has yet to materialize. For the most part the push for smart cards as a stored value, e-purse, or to secure online shopping purchases has seen a "lukewarm" response at best. Lately, smart cards have been positioned as "cool gadgets" to carry with the potential to offer numerous value-added benefits. That, says Celent, is doomed to fail as well.

"Smart card usage continues to flourish in Europe," comments Meredith Hickman Outwater, author of the report. "But without a serious problem to solve, such as fraud reduction, or consensus from a major banking consortium to transition in unison, smart cards are expected to languish in the U.S. market."

Privacy Management Becomes More Hazardous

A report card issued by USAction, a national consumer organization, found that bank privacy notices are confusing and misleading and fail to comply with the new federal law.

"All financial institution's must work harder to put privacy management on the front burner all the time or it will come back to bite them in the wallet."

USAction graded the privacy notifications sent out by the 15 banks that issue the most credit cards and found that three received an "F," six got a "D" and no bank got better than a "C."

Given banks' track record with privacy notices and faced with, what Meridien Research describes as, "A complex web of operational business processes, marketing, and international/cross-border compliance."

Financial institutions must learn to effectively deal with the privacy issue. "Consumer beware, when a bank says 'Your privacy is important to us' hold on to your wallets," says William McNary, president of USAction in an organizations statement.

"Bank privacy notices are designed to be confusing and misleading in order to convince consumers not to exercise even the very weak privacy protections available under the law…it's no wonder that consumers shake their heads at the hard-to-read notices and throw them in the trash rather than acting to protect their privacy," adds William.

All financial institution's must work harder to put privacy management on the front burner all the time or it will come back to bite them in the wallet.

