Introduction

JPMorgan Chase is the largest provider of US dollar (USD) clearing services and provides nondollar payment and clearing services worldwide. Disaster recovery and payments system contingency have been top priorities for both JPMorgan Chase and its predecessor banks for more than a decade. Since the merger, JPMorgan Chase has consolidated its high-value payments processing operations to meet business and firm-wide strategic goals and now provides among the highest level of back-up and business continuity preparedness in the industry.

The bank views disaster preparedness as critical not only to its own payments business, but also to its counterparties, the high-dollar payments industry, and to critical financial markets. On and after September 11, 2001, JPMorgan Chase was able to continue uninterrupted payments processing—assisting less fortunate customers and counterparties through advice, alternate payments routing, and use of bank facilities and technology, as well as injecting needed liquidity into the market. Today the bank’s payment services satisfy or exceed the points raised in the regulators’ Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.
This TowerGroup Research Note looks at the business continuity services for high-value payment clearing at JPMorgan Treasury Services and best practices being implemented by the bank. (For related research on wholesale high-value payments systems resiliency issues, refer to TowerGroup Research Notes 033:25PWF, “Emerging Factors in Wholesale Payments System Resiliency in the US,” and 034:04P, “Resiliency for High-Value Payments Processing in the US: New Models Needed?”)

**Background**

With year-end 2002 assets of US$759 billion and business in more than 36 nations, JPMorgan Chase is a major player in global trade and financial markets. The firm is the second largest domestic bank holding company and is a leader in US dollar and cross-border payments through its JPMorgan Treasury Services organization (subsequently referred to as Treasury Services). Treasury Services provides treasury, cash management, trade finance, and e-commerce services to financial institutions, companies, and government and other entities worldwide.

Within Treasury Services, the Global Clearing business unit (subsequently referred to as Clearing) is responsible for all high-value clearing. On an average day, the bank clears more than 230,000 wire payments valued at close to $1.4 trillion, at a 95% straight through processing (STP) rate. The business supports close to 4,500 correspondent relationships and more than 7,000 corporate customers, including the 50 largest global banks and 70% of the US Forbes’ 500, respectively.

The Clearing unit has been recognized for its leadership position by citations in 2001 that include:

- Number 1 in USD treasury clearing and commercial payments (*FIMetrics, September 2001*)
- Number 1 in CHIPS, Fedwire, book transfer volume (*Ernst & Young Cash Management Services Study*)
- Highest CHIPS average daily volumes (*The New York Clearing House, Q4 2001*)
- Highest Fedwire average daily volumes (*The Federal Reserve Bank of New York, Q4 2001*)

The Global Clearing business unit has recently completed consolidation of its business operations to Florida and has more than 550 business management, operations, customer support, applications development, risk management, and other support staff at the Treasury Services’ Tampa-based campus. The business unit also retains a major presence in New York City, which includes product management and other business professionals. This division manages multicurrency clearing through its global operations, primarily in Europe and Asia.

Operational risk management, disaster recovery preparedness, and business continuity planning for payment clearing are vital to the viability of the business and the bank. The quality of service delivered to customers and counterparties is dependent on the resiliency of its payments infrastructure and its people. In 2002, Clearing invested more than US$10 million for operational risk and disaster preparedness.

**Payments Systems Resilience**

Firms such as JPMorgan Chase that are significant players in critical financial markets are facing new challenges to increase the resiliency of their high-value payments processing business. The emerging requirements of the New Basel Capital Accord (Basel II) and new domestic supervisory expectations outlined in the *Sound Practices* white paper dictate that banks control operational risk more effectively to reduce the potential for disaster and to be able to recover and resume payments processing within tighter...
timeframes if a disaster takes place. The white paper requires banks to diversify their payments processing business across systems and geographies. Also, since 9/11, customers, payments systems operators, other financial institutions, and industry entities are driving development of more robust contingency capabilities. These forces will have a sizeable impact on a bank’s people, business processes, and technology strategies, as well as on how the bank manages relationships with critical nonbank infrastructures and other external service providers.

Treasury Services is playing a major role in payments systems resilience developments. The bank is a member of The Clearing House and a leading member in the Clearing House Inter-bank Payments System (CHIPS). Treasury Services executives co-chair the Federal Reserve Bank’s Payments Risk Committee and sit on the SWIFT Board of Directors. Clearing also participates in the Banking Industry Technology Secretariat (BITS), the Financial Services Technology Consortium (FSTC), and related forums and activities.

**The Global Clearing Model for Business Continuity**

JPMorgan Chase is addressing these demands on multiple levels. At the highest level, the bank has established business continuity and risk management standards for the corporation as a whole. These standards on operational risk management and disaster preparedness are then fleshed out in detailed plans and procedures for each line of business, physical location (buildings or campus), and the information technology (IT) organization. (See Exhibit 1.) The firm takes continuity very seriously and has developed a structure to ensure success. Both business and IT units are measured on the quality of their preparedness, resilience, and compliance to standards.

---

**Exhibit 1**

**JPMorgan Business Continuity Model**

The Global Clearing business unit has overall responsibility for the continuity of its business. Its business continuity plans encompass all aspects of its business processes, including business operations and data centers/information technology. Although it functions under the business continuity policies for Treasury Services at its Tampa-based operations campus and under IT contingency objectives, Clearing manages
all risk, recovery, and resumption decisions in the specific context of its payments processing and clearing strategies.

A dedicated team, the Business Emergency Office (BEO) manages all aspects of emergency and disaster preparedness at the Tampa campus. The BEO is responsible for onsite preparedness and offsite contingency services and works in conjunction with the resident Treasury Services business units on training, facilities, infrastructure, and relocation decisions. Clearing works closely with the BEO to ensure that its programs and procedures support the mission-critical needs of Clearing’s business and its people. On the technology side, JPMorgan’s corporate Enterprise Technology Services group (ETS), which is part of the IT organization, manages the data centers that support its payment clearing business. Here again, however, Clearing determines how its business must be supported and sets specific objectives for ETS’s support of its systems and applications. Exhibit 2 highlights selected facets of business operations and data center disaster preparedness for the US-based business.

Exhibit 2
Clearing’s Business Continuity Responsibility

<table>
<thead>
<tr>
<th>Category</th>
<th>Business Operations</th>
<th>Data Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities Management</td>
<td>Location-specific: Business Emergency Office (BEO)</td>
<td>Enterprise Technology Services (ETS)</td>
</tr>
<tr>
<td>Disaster Recovery (DR) Site Management</td>
<td>Clearing owns and manages</td>
<td>ETS</td>
</tr>
<tr>
<td>Clearing Objectives</td>
<td>No downtime with immediate recovery other processing sites</td>
<td>2-hour recovery: backed by real-time data mirroring to second site and multihop to third site</td>
</tr>
<tr>
<td>Training</td>
<td>Contingency training: BEO team; Functional cross-training: Clearing</td>
<td>Application training by vendor or internal development team</td>
</tr>
<tr>
<td>Implementation</td>
<td>As-needed by Clearing under strict change control management</td>
<td>As-needed by Clearing under strict change control management</td>
</tr>
<tr>
<td>Testing</td>
<td>Bimonthly site contingency tests</td>
<td>Annual site testing</td>
</tr>
<tr>
<td></td>
<td>Semiannual &amp; quarterly tests with clearing &amp; settlement systems</td>
<td>Semiannual component testing specifically for Clearing</td>
</tr>
<tr>
<td>Disaster notifications</td>
<td>Customer notifications and internal escalations to executive management</td>
<td>Vendor and service provider notifications</td>
</tr>
<tr>
<td>Critical Documents</td>
<td>Daily replication to DR site, with Web-based access; business continuity plans and procedures on JPMorgan intranet</td>
<td>Escalation procedures and contact data available at DR site</td>
</tr>
</tbody>
</table>

Source: JPMorgan Treasury Services

Business Continuity Plan
Business continuity for Clearing is as much an ongoing process as a plan. There are, however, actionable people, site, and systems plans that encompass processing, application, and system recovery and resumption goals as well as customer notification and crisis communication procedures. The documented plans detail
critical activities and the response for any level of outage or emergency condition and includes basic emergency, electrical power, water and sanitation, telecomm services, recovery facilities, transportation, and vendor and service provider support arrangements. The plan includes identification of critical staff and the roles and responsibilities of all staff during a crisis. Plans are then integrated with other JPMorgan plans as appropriate. All staff is trained, and exercises are held to test various emergency scenarios.

Investments in continuity are developed to provide ongoing benefits for the business—not just to provide a multimillion-dollar disaster recovery capability. This means that operations and technology decisions made for business continuity must also bring practical efficiencies to business processes and the day-to-day business operation. The strategy has helped Clearing to gain the cost and business process efficiencies inherent in consolidated operations while diversifying its access, customer service, and risk across several geographies and time zones.

Defining Disaster

A key facet of disaster preparedness is being able to determine the scope and criticality of an event and how to react to it. This requires advanced planning including definition of potential scenarios and responses and invocation of the business continuity plan based on a judgment of the event. Although September 11 has captured the industry mindset, most events are much less clear-cut. Many operational or outage conditions, while severe, don’t require implementation of the full plan. And too rapid a declaration of disaster can set in play processes that might turn out to be unnecessary. Timing is also critical to an event’s importance. Treasury Services uses Severity Level planning to frame its reaction to an event. As shown in Exhibit 3, each level has its own criteria. Each also triggers a preset series of explicit actions and event management procedures that determine the depth and timing of the business unit’s response. (It should be noted that the data centers use a similar framework to manage outages, although the response for most outages is immediate, onsite, and hardware or network related.)

Exhibit 3
Severity Level Planning for Global Clearing

- Localized damage
- Critical functions relocated onsite
- 30-minute horizon for resumption
- Severe damage to primary operations
- Interrupted processing
- BEO decision on removal to recovery (DR) site
- Extensive damage to primary site
- Critical staff relocated to DR site
- Event severity determines duration of DR site processing & need for full staff relocation

Source: TowerGroup
Operational Risk Management

JPMorgan’s corporate risk management framework is the foundation for line of business operational risk management programs. Located with the business unit, dedicated risk managers help identify, manage, and mitigate business risks and work in concert with Clearing’s management to develop measurable and actionable operational risk indicators and metrics. The operational risk model provides tools and practices to create a capital framework that can be integrated with payments business initiatives. Tools range from risk assessment matrices to new product and technology risk management reviews. Key to the model is Horizon, a JPMorgan-developed Web-based risk management tool used by Clearing (and other business units) to manage operational risk through self-assessment, measurement, audit testing, and action plans.

Horizon also plays a role in business continuity and contingency planning by compelling managers to regularly review and assess the effectiveness of their business practices in these vital areas. Similarly, key risk indicators (KRIs) are established, tracked, and tested to provide an analysis of how well the business performs, and complements the completeness of its recovery and business continuity plans. (Exhibit 4 highlights selected KRIs for Clearing.) Horizon includes a checklist for appraising business processes and the preparedness needed for each function based on its importance to the business. Business unit performance is tracked to established metrics as part of a capital incentives program. The Clearing unit has consistently met its targets and will be increasing self-assessments from semiannually to quarterly in 2003 to augment performance further.

Exhibit 4
Selected Key Risk Indicators for Clearing

CUSTOMER SERVICE
- Same-day response rates
- Transaction : inquiry ratio
- 3-day and/or 5-day resolution rates

PAYMENTS PROCESSING
- Straight-through rate
- Payments errors per 1,000
- Significant system outages (downtime)
- Claims
- Turnover

Solving Substantial Preparedness Issues

Clearing’s continuity model is leading industry best practices for payments clearing. Today the bank satisfies or exceeds virtually all of the sound practice recommendations set out in the US interagency white paper and is continuing to evolve its disaster preparedness to meet emerging requirements.
Tertiary Processing Strategy

Clearing has adopted a tertiary process strategy that is the core of its payment clearing operational efficiency and business continuity. This tertiary model makes JPMorgan Chase one of only a few US banks that will have three active “split operations” sites in 2003. The model is part of Clearing’s payments consolidation strategy to integrate what were previously discrete processing units in Asia, the US, and the UK into a central three-tiered hub supported by regional satellite processing centers. (See Exhibit 5.) Clearing refers to its model as meshed processing, which the bank has structured as a split-operations model, with processing in Tampa and the UK. (The third site, now the US recovery site, will be active this year.) Tampa does the bulk of the processing given the size of its USD clearing business, but there is already some shared cross-currency processing for Asia, Europe, the Middle East, and Africa in Tampa and for USD clearing in the UK.

Full occupancy of its US-based disaster recovery site in 2003 will provide Clearing with three “hot” sites and ensure virtually uninterrupted processing even with a disaster to a primary operations center. The tertiary site houses a smaller permanent staff than the other sites, but it places operations staff at a third physical location and supports space to house the US primary site staff in the event of an evacuation.

The model is already delivering substantial benefit to the business. It ensures seamless, continuous processing across continents and time zones, providing a simultaneous window into payments clearing for the entire business. Multiprocessing locations also allow the bank to maximize the processing day for both US-based and offshore customers. This could prove especially useful when the Federal Reserve lengthens its processing day in 2004, with a 9:00 p.m. opening, given the number of bank clients in Asia and Europe. The strategy also facilitates deployment of new technologies, particularly those related to STP throughput, automated inquiry, investigation, and repair. In addition, the model allows the bank to provide 24/7 support to corporates and correspondents through customer service units located on four continents.

Best Practices

Best practices instituted to date cross four broad categories (summarized in Exhibit 6).
Best Practice Areas for Global Clearing

| √ | Critical activities | Achieved through Horizon KRIs, Severity Level framework, and contingency plans |
|   | Dual site strategy | Tertiary “split operations” strategy backed by three sets of dual data centers for the core processing system and clearing systems interfaces |
| √ | Separation of business operations & data centers | Separated by geography and management |
| √ | High levels of redundancy | Onsite relocation for business operations and onsite recovery for data center hardware and software; three staffed active operations facilities with independent cross-trained labor pools; tested network redundancy to clearing & settlement systems; back-up internal network paths; multi-tiered data back-up and management |

Source: TowerGroup

Critical Activities. Clearing defines critical activities in several ways. Key risk indicators and super KRIs are set up in concert with Horizon. New business, new product development, and regulatory requirements are all factored into the assessment. The Severity Level framework and business continuity plans document management and timing targets for each activity, where the end goals are staff safety, continuous processing, and high availability to customers. Business operations, the BEO (or similar group), and the data centers each have unique critical activities.

Critical processing activities are tested on a consistent basis and encompass end-to-end tests with the clearing and settlement networks, customers, counterparties, and others. JPM’s internal business audit is continuous, and there are annual audits by the Federal Reserve and state governments. (The UK Business Operations is subject to the same type, though not the same quantity, of audits.) Data center critical activities have a similar standard testing cycle, and the critical infrastructures at site facilities are tested on a weekly basis.

Dual Operations and Data Centers Strategy. Operations and data center facilities for the Clearing business conform to split operations and dual data center site strategies laid out by regulators. The tertiary operations model moves beyond the recommended Sound Practices split operations model. Each major core processing system is supported at a primary and back-up data center—making a total of five key centers that support the payment clearing business. Each Clearing processing and IT facility, respectively, draws on a unique labor pool. Facilities are on different power grids and have multiple telecomm carriers with redundant network paths, independent water supplies, and multiple transportation alternatives. Each facility also has its own generators, which are tested regularly and are auto-triggered by a three-second outage. Security at facilities is high and is upgraded as appropriate.

Separation of Operations and Data Centers. Clearing’s processing and data centers facilities are separated by system and region. Although there had been some overlap in the past, today none of the major sites houses both operations and IT personnel.
High Level of Redundancy. A high level of redundancy is evident in all areas: people, process, technology, and critical infrastructures. The Tampa Business Operations campus includes about 100 operations and 150 customer service staff, and the UK and tertiary sites add another 200 people. High-speed technology and sophisticated artificial intelligence afford Clearing with 95% straight through processing rates. This automates the majority of the activity. Geographically dispersed data centers handle the bulk of the transactions automatically. The remaining transactions, exception processing and customer service, are handled by Clearing staff.

Business Operations staffs are categorized as nonessential, essential, or critical personnel. With close to 60% of the staff designated as critical, people are a major consideration for the business. Treasury Services has invested in a cross-training program and is initiating new workday programs and schedules to the extent possible. Business management for Clearing is also separated along geographic lines for business and redundancy purposes. Even with the Tampa consolidation, senior business and technology executives are housed in New York City and elsewhere.

Security for the processing and data centers is high and consistently monitored. There is a high level of immediate onsite redundancy for Business Operations, so that relocation to a recovery site is necessary only in a worst-case situation. The Tampa campus, as an example, has a state-of-the-art training facility that permits onsite “within minutes” relocation backup. Alternate telecomm and technology infrastructures are continuously available and ready. The bank met with telecomm service providers immediately after 9/11 to test written guarantees of redundancy of lines and network connections for the processing facilities.

Clearing’s products are supported at multiple data centers in both the US and the UK. Each of the major core payments processing and messaging systems is sited at both primary and back-up data centers, although data center locations are different depending on the system. None of the data centers share the same telecommunication infrastructures or power grids.

Offsite access to all documentation, notification and contact lists, and emergency procedures, as well as the business continuity plan is available over the Web.

Working with Customers and Counterparties

Although Clearing has had an ongoing dialogue with major customers relative to business continuity issues, 9/11 naturally increased customer interest. Many customers are hard-pressed to keep up continuity issues—from an expertise as well as a technology view—and are looking to outsource to the bank. The bank is promoting its Treasury Readiness program as a way for corporate treasurers to learn how to better protect their business and to increase the number of customers that have viable contingency plans, at least for the aspects of their business that affect the JPMorgan relationship. For its larger corporate customers and correspondents, Clearing is promoting end-to-end contingency testing, including back-up-to-back-up systems, and it is sharing aspects of its own contingency plans as the need arises.

This is true also for counterparties with which the unit does a significant amount of business. The Federal Reserve Bank (and the other agencies) wants major financial institutions to share key contact information to reduce vulnerabilities in high-value payments systems and critical markets. A significant issue here is connecting cross-market industry groups (cash, commercial paper, securities) to resolve continuity problems. Clearing is engaged with industry counterparties on these issues. Although practical implementation will be difficult to achieve, it is nonetheless a necessity for the industry.

Planned activities include using existing Web-based and electronic banking products or its new online Notification Request advising service (part of the eServe product) to provide outage or disaster-related
notifications. The Notification Request service is e-mail-based, using push-technology to provide customers with time-driven event information according to customer-established criteria. It could be used in disaster situations to provide critical information and payments data and advise customers, and, optionally, their beneficiaries, via PCs and laptops, personal digital assistants (PDAs), alphanumeric pagers, and wireless phones.

**September 11, 2001: A Case in Point**

At the time of the September 11 disaster, the Global Clearing business unit was in the final stages of consolidating its operations from New York City to Tampa with 70% of its staff already on the ground in its new facilities. The Clearing organization did not lose a single staff member and was able to continue processing high-value payments without interruption during the event. In fact, the greatest strain on the organization lay not with its own people and systems but in dealing with external parties: Managing communications with the payments systems operations, regulators, and service providers, as well as assisting clients affected by the disaster took its toll on Business Operations’ resources and normal support activities. The bank supported more than a dozen less fortunate correspondents (one for nine months), providing space, technology, and processing services, and worked continuously with corporate customers throughout, and after, the event. The bank was also able to offer services to customers of other large banks that experienced difficulties, clearing $1.939 trillion in USD wire transfers during the crisis period and injecting millions of dollars into the payments system to help maintain market liquidity.

**Moving on from 9/11**

Since 9/11, Clearing has focused primarily on business operations improvements. The bank has placed loss of life and staff safety issues at the top of its business continuity agenda. Issues such as emotional trauma and family relocation are being incorporated into the business continuity plan. Dispersal of resources among diverse facilities, working from home, cross-training, and flexible work schedules are all being examined. While Treasury Services has not capitalized on its disaster recovery effectiveness during the crisis, the business has clearly benefited from its ability to provide ongoing high-value payment clearing services during the disaster.

**Key Payments Technologies**

A major advantage of business operations consolidation is that the same processing platform is used to support the business globally. The unit has taken a buy-and-build approach to payments technology, combining all applications in an integrated architecture. Front-end applications used for connection to the clearing and settlement systems and SWIFT are vendor-supplied. There is a mix of vendors and platforms because Treasury Services does not want all its mission-critical systems consolidated with a single provider. The platforms chosen, however, all support the resiliency requirements of the business. The engine for payments processing is the proprietary Global Funds Processor (GFP) application, which is deployed on multiple IBM processors. GFP is the core processing engine for payment clearing and manages all processing activities for Clearing’s 230,000 average daily transactions. (The system has the capacity to handle more than twice that volume on a peak day.) GFP is supported by two other homegrown systems, Global Data Capture (GDC) and Global Funds Control (GFC). GDC manages the front-end feeds from customer access and internal systems into GFP, and GFC provides individual customer position management.

Clearing uses a vendor product as a core platform to automate investigations and inquiry management functions. A proprietary software application is used to increase its repair and STP rates. The Artificial Intelligence Repair Server (AIRS) uses intelligent technology to identify and correct recurring patterns of
errors in messages—arising, for example, from incorrect data or outdated repetitive lines in incoming wires. Enhanced Acronym Search Engine (EASE) corrects credit bank information that allows the system to route the transfer accurately. Both technologies help in disaster situations by increasing STP and reducing the number of work-in-process items.

Clearing is extending its capabilities for multi-tiered data mirroring and management. In addition to synchronous mirroring of payment transaction data from primary to back-up databases, Clearing is replicating end-of-day payments and related cash transactions via a bulk transmission to storage management systems. The bank is also investigating use of multihop technology to replicate data across long distances to a tertiary site to accommodate greater distance as well as use of synchronous vaulting to intermediary sites to safeguard less mission-critical data that might be needed under a prolonged outage or disaster situation.

Looking Toward the Future

Clearing will complete its strategic consolidation and business continuity preparedness during 2003. New strategic efforts will center on industry-wide initiatives related to payments systems risk reduction and cross-industry efforts to ensure transparency of critical infrastructures in the event of regional or more widespread disasters. In this regard, Treasury Services will continue to work with the federal agencies to ensure safety for the business and USD liquidity. Treasury Services is also part of a firm-wide Corporate Security Council that will focus on employee preparedness, safety, and facilities.

Clearing continues to build out its business continuity model as part of its overall strategies for the business. It will continue to evolve the tertiary model and the demands of payments (volume) processing distribution across the three hubs. Technology investments will center on those that increase throughput and STP rates toward 98%, lower risk, and provide operational efficiency and resiliency gains. They range from greater use of artificial intelligence technologies for repair and automated interfaces with internal systems, to customer self-service products, to replication technologies and advanced storage management solutions. Concurrently, business-related initiatives will increase. Significant efforts will be spent working with customers on preparedness and operational risk issues. Increasing the sales of Horizon is a key component of this strategy: It not only provides revenue to the bottom line, but also helps move customers toward a JPMorgan Chase standard for operation risk management. Clearing will also conduct extensive end-to-end testing (including back-up-to-back-up systems) between and among wholesale payments systems, counterparties, and customers and continue to augment its own scenario and rapid response planning.

Conclusion

The Global Clearing business unit is positioning to extend its lead in USD and other cross-border high-value payment clearing. It views disaster preparedness and business continuity as critical components of its payment clearing business strategy and has made a multimillion-dollar commitment to provide the highest level of business continuity services. To date, investment has paid off in its ability to accommodate new regulatory expectations without changing strategic business direction or making substantial unplanned expenditures. Ironically, the firm’s focus on risk management and business continuity that once frustrated its sales and marketing staff is today a major factor in attracting new payment clearing business. Global Clearing is banking on the expectation that correspondents and large corporate customers will increase payments volume (and value) commitments in return for iron-clad assurance of payment execution and clearing. The challenge for the Global Clearing business is to continue development and refinement of
its hub model to achieve the desired operational efficiencies and attract new business commensurate with its investment and business continuity goals. The challenge for other banks without comparable resources to invest is to achieve a similar level of contingency. At the high end of the payments clearing market, the number of banks that can compete easily with new regulatory demands is not a large one.