Managing Financial Network Mandate Testing

An old adage says "Nothing is certain but death and taxes," but for testers in the financial industry, network mandates are just as inevitable—however, they need not be as unwelcome. Careful planning can make creating test plans for network mandates more efficient and less stressful.

What *is* a network mandate?

In financial testing, in its simplest terms, a ***network mandate*** is a financial network's periodic notification of upcoming mandatory changes to the procedures currently in place for its members. Members must be in compliance with these mandates by a specified date. For the purposes of this article, a ***network*** is a term used to refer to international, national, or regional entities that have members participating in the use of a common card type or network (switching or interchange) service, such as MasterCard, Visa, American Express, Pulse, Plus, STAR, etc . Some of the information here will apply more directly to switch networks, or card associations, or network processors, and some topics may apply universally. Ideally, you'll be able to use this information to start developing a mandate test plan that meets your organization's specific needs.

Mandates encompass many types of changes. For example, changes may be related to:

- **Products** - New cards or transactions being supported
- **Processing requirements** - Changes to processing by issuers or acquirers, or notification of additional processing requirements for all network members
- **Message formats** - New or expanded fields, or specific content requirements for those fields
- **Batch processing -** New fields, or new data for existing fields
- **Reports**– New reports, or additional information requirements in existing reports
- **Business practices or network rules** (that may not affect system processing) – Network logo changes that result in changes to its members' signage, or changes to legal documents related to network participation

How am I supposed to test all this?!?

A formidable stack of paper lands on your desk with a sticky note directing you to "Test this." It's easy to feel overwhelmed when faced with such a daunting task. Like that proverbial journey of one thousand miles, though, testing the changes required to bring your organization into compliance with network mandates is a matter of completing one step at a time.

Getting the mandates in hand

For some testers, the first obstacle is *finding* the mandates. Mandates may be distributed to others in your organization. Communicate to the mandate recipients that you need to analyze the mandates as soon as possible to begin planning tests. Although often mandates are updated and revised by the association before being finalized, you can still begin a testing requirements analysis, and then revise your plan as further details become available.

Analyzing the mandates

When you receive the financial network mandates, your first task is familiarizing yourself with them. Begin preplanning by asking yourself basic questions such as:

Which items actually *apply* to my organization? For example, some items apply only to certain transactions, products, or account types. Some apply only to issuers, or acquirers, or processors. By determining which items apply to your organization, you can reduce the number of items (and pages!) that you must focus on when creating your test plan.

Which items actually require *testing*? Is testing required for your online systems *and* batch systems? As mentioned previously, some items (for example, updates to legal documents, changes to logos, etc.) require action by others in your organization, but do not require testing. Scan the mandates for items that directly affect processing or processing output (fees, reports, batch files, and so forth). Note any items you are uncertain of; for example, will chargeback processing require in-house testing or not?

Pay special attention to any online changes that may affect back-end processing (also called *clearing and settlement*, or *reconciliation* processing) and discuss these changes with coworkers who specialize in this processing. Their input is crucial to guarantee successful end-to-end processing in your system. Changes to back-end processing are easily missed, and normally you are not required to certify this processing with the network. The result can be a scramble to institute last-minute fixes to handle changes to back-end processing *after* the mandates are put into place.

By asking for reconciliation files—as well as network reports—for the online transactions performed, you can avoid any unexpected complications. Try to include some regression testing during the online certification process to provide a more robust end-to-end testing scenario.

What is the deadline for compliance? Mandates provide not only the changes required, but the dates by which those changes must be completed and verified. Your organization must evaluate the impact of the mandates, determine the resources required to make the changes, and plan accordingly. Your test plan must take these deadlines into account as well.

Is live testing with a switch required, or is in-house testing sufficient? Are you required to provide test results that prove your organization's compliance? Some networks will require live testing (sometimes called *certification testing*) through a connection with the switch. It is critical to note which items require live testing, then work with your developers to determine when the required code changes can be completed so you can reserve your test time. Most switches have many members—all needing to certify their mandated changes. Test time is limited, and sometimes expensive. While you don't want to risk paying for test time that you cannot use effectively, your organization must weigh those expenses against the penalties or fees charged for noncompliance by the specified date.

Which items are mandatory and which are optional? Which items are optional *now*, but will be mandatory in the near future? "Mandates" may be a misnomer because, in fact, not *all* mandates are mandatory.

Consulting other experts

After you've made your initial pass through the mandates, you will undoubtedly have questions. Look to internal experts within your organization—such as network liaisons, developers, and others—for assistance. Typically, your internal experts can help you address issues such as:

- You need to review the specifications for changes related to a mandated item.
- You need more information on the existing processes (products, messages, etc.).
- You need to clarify if an item does or doesn't affect processing.
- You need to develop testing for an item that affects multiple aspects of processing.
- You need to become more familiar with the affected processing task before you can develop an effective test plan.

In addition to your experts on staff, you can also work with experts outside of your organization, such as software vendors.

Pre-testing activities

After you've analyzed the mandates, you will likely have noted some activities that you can begin even before your test plan is completed.

- Assembling test accounts, cards, and data
  Your testing may require specific test plastics, test card data, or test accounts. For magnetic stripe card testing, you may need specific track data; and for EMV card testing, you may need cards with specific applications. You may also need PINs and CVC data for your test cards.

- Preparing for live testing
  If live testing is required with your network, you may need to resolve any communications issues related to establishing connectivity, and you will need to agree upon a test script or test bed, or exchange test

data with the network. Try to get these housekeeping matters settled before certification testing begins, rather than wasting your limited test time trying to resolve them.

- Locating software to aid test efforts
  First, be sure to check with developers for any automated test tools they may use during development. In addition, your organization may have other tools that could make testing easier for you, even though these tools may not be classified as "test tools." These may include editors for posting and log files, viewers for report data, and programs for auditing incoming and outgoing messages.

What do I include in my network mandate test plan?

In a perfect world, every organization could use one "standard" test plan to test mandates. In fact, every organization has different implementation issues, a different collection of products and transactions supported, varied roles (issuer, acquirer, or processor), and so forth. Similarly, each mandate has specific requirements that affect different system processes.

Fortunately, although every tester has a favorite approach to test plan development, there are some commonalities. Developing any test plan means first deciding what testing is required (what processes to include and exclude) and then deciding how to test the included processes (writing the test scenarios and scripts). After the test plan is developed, it should be reviewed by peers (other testers or developers), and possibly by other system users.

Baseline testing

Before you can begin testing changes required by the mandate, you need to run baseline tests. Baseline tests serve to document how the system performed *before* any mandated changes were applied. If you test only the updated code, you are unable to ensure that a "fix" related to compliance with a mandated item did not inadvertently break something else. Comparing the output and test results from the baseline testing with the output and test results from the updated code enables you to verify that the existing code functions as it did previously, and becomes the first step in ensuring that the updated code successfully adds the function for which it was designed.

Testing requirements

The test cycle involves running and documenting tests on the updated code, reporting bugs during testing, and reporting any other anomalies between the results (or output) from your baseline tests and the results (or output) from testing of the updated code.

Though test plans are different, generally testing requires:

- Viewing the log files (including input and output log files) to make sure that transactions are logged correctly and the appropriate data is stored

Are transactions logged completely? Are there unexpected errors indicated by the journal or log that need to be investigated? Does journal file data and reconciliation file data correspond? Are "suspect" transactions noted (but assets unaffected)? Are message responses generated correctly? Do downstream processes reflect online testing?

- Verifying that all endpoints are affected as desired
  Does the posting and reconciliation system correctly reflect testing? Do batch files and reports correctly reflect the expected test results?

- Verifying cardholder accounts are updated correctly
  Are accounts debited or credited appropriately? Is the transaction data recorded as expected in the logging applications?

- Verifying the reversal processing
  Do account totals reflect reversals or partial reversals? Are reversed transactions correctly recorded by the system? The system must include the original transaction data as well as the reversal of that transaction. For partial reversals, ensure the system correctly reflects any applicable overage or shortage.

- Scheduling meetings to report and resolve issues
  Do you have processes in place for reporting and resolving issues discovered during testing? Early during your testing, establish a schedule of meetings with developers (and other personnel, if needed) to discuss issues and possible solutions or workarounds. Remember to include clearing and settlement, reconciliation, or other personnel involved in "back-office" processes. The number of issues will determine the frequency of these meetings.

- Performing negative tests
  Is invalid input handled correctly? Does the system recognize invalid data elements? Are invalid messages declined without affecting system performance? Can the system handle declines, rejects, and denials correctly?

- Performing regression testing (to test existing functionality)
  Do existing transactions continue to flow as expected? Do reports and batch files continue to reflect all client activity?
  Regression testing is a combination of science and art. All testers realize you cannot test the *entire* system. The hallmark of good QA or QC test planners is their ability to determine the areas of the system in which errors could result in the highest risk to the organization and rigorously test those areas, and

then supplement those tests with broader-spectrum testing designed to adequately test areas where errors present lower risk. An organization's regression testing framework must grow to encompass recent changes to the system.
For example, a regression test plan for testing changes to withdrawal transaction processing means not only testing withdrawals from various account types (checking and savings), but also testing withdrawals with cash back, and withdrawals conducted with and without a PIN—and then testing a number of other similar transactions.

- In some cases, stress testing (to test your system's load capacity)
  Some changes (for example, mandated EMV support) may translate into additional processing overhead. For these mandates, stress testing may be advisable to ensure your processing system can support your anticipated transaction volume.

More tests in less time: automated test tools

You have seen that planning can make network mandate testing more manageable, but are there ways to test ***more*** scenarios and test them ***faster*** than you are now? For many organizations, automated test tools are a means of increasing not only testing efficiency (particularly as opposed to manual testing with physical cards and terminals), but also of improving the thoroughness of test plans. Testing faster means you have time to complete a wider range and greater number of test scenarios—scenarios that would not have been possible previously. Your organization can realize significant time (and cost) savings by moving to automated testing—not only for testing changes related to compliance with network mandates, but any time testing is required.

About Paragon Application Systems

Paragon Application Systems is a leading global provider of ePayment simulation, configuration and testing software tools to the financial industry. More than 400 financial institutions in over 80 countries use Paragon tools to improve quality and reduce time-to-market. Paragon's broad customer base includes major interchanges, processors, leading software providers, banks and credit unions. Visit Paragon Application Systems at www.paragonedge.com.

About the Author

Lynn Tjepkema, ePayment Specialist in Paragon's Professional Services department, is responsible for analyzing customer requests and developing working solutions to address testing needs. Lynn is ISTQB certified and has over 20 years of software development and testing experience in the financial services industry. She has extensive knowledge of financial network message protocols as well as authorization and settlement processing, with special emphasis on Visa, MasterCard and American Express.