

GROWTH IN PAYMENT RISK CAN BE MITIGATED!

2/17/2009

Using Technology to Mitigate RDC Risk



Written by Eston Fain

Director of Opritech, a Division of AQ2 Technologies, LLC

*AQ2 Technologies, LLC
135 Gemini Circle, Suite 204
Birmingham, AL 35244*

Growth in Payment Risk Can Be Mitigated!

USING TECHNOLOGY TO MITIGATE RDC RISK

INTRODUCTION

The banking experience for small business owners is changing. Conveniences are finally here that do away with one chore that is no fun at the end of the day - getting the day's deposits to the bank. It is no wonder that business owners want to eliminate making deposits in bad weather or in high risk locations and at night, but they are also facing resource shortages in a tightening economy where cash flow is becoming increasingly important. Small businesses are quickly adopting technology and services that allow them to make remotely captured deposits to their bank.

The question for banks is who the small business owners will use to gather and send their deposits to the bank. There are a growing number of payment aggregators, aggressive financial institutions, and companies that provide bank agnostic deposit services entering the market. These players are deploying sales teams to provide scanners as part of their merchant services package. In some cases, checks as a "merchant-preferred" payment method are cheaper to process adding more value to the merchant for these services.

Remote Deposit Capture (RDC) provides the way to gather deposits but also represents new payment risks to banks accepting these deposits with this new technology. Remote capture expands the sources of deposits beyond bank controlled desk top scanners to fax machines, home and office scanners, and even cell phones with digital cameras. ISO's (Independent Service Organizations) are providing the latest expansion of remote deposit technologies. Offering remote deposit capture as a merchant service, the ISO's have expanded RDC beyond a bank's normal service offering to corporate customers. These new remote depositors present unknown or unacceptable risk potential to financial institutions that incorporate basic risk analysis and detection methods. Simply providing duplicate detection, MICR verification, and per-deposit limits are no longer adequate to protect banks, especially where customers submit deposits from multiple locations or through multiple sources.

The need for such deposit scrutiny is identified in the January 2009 FFIEC Guidance document labeled "Risk Management of Remote Deposit Capture". The FFIEC is telling banks that you can "Trust the depositor" but you should "analyze each and every deposit" as a rule.

The industry requires innovative and automated methods of analyzing the deposits to enforce the new guidelines and provide strict control of depository and merchant agreements made between the financial institutions, aggregators and business owners of all sizes.

TECHNOLOGY ENABLED RISK MITIGATION

RDC, as the FFIEC notes, is a new delivery system with its own set of legal, compliance, market, and operational risks. As organizations assess the risks of RDC and define high level risk management processes, banks and aggregators are coming to the conclusion that the identification, assessment, control, and the measuring and monitoring of RDC is much more than duplicate detection and MICR validation. The industry is beginning to realize that comprehensive risk control will require new, technology enabled solutions to be effective.

Financial Institutions need a risk mitigation solution that allows them to set rules to monitor and enforce the depository, merchant, and internal risk policies established with its customers. This includes tracking the

number of daily deposits, deposit amounts per period (days, weeks, months or years), item amount limits, item count limits and other parameters. Furthermore, they need tools that are flexible enough to match risk monitoring requirements in “profiles” to specific risk threats, to relationship cycles, and even to individual customers in some cases. Monitoring customers with a profile of rules that can aggregate levels of dollar limits or debit counts enables the bank to determine the level of risk it is willing to accept per depositor or, for instance, at the store level of a multi-store depositor, as well as consumer customers.

A risk mitigation solution must be able to differentiate between new relationships and established accounts. The solution must provide profiles containing more stringent rules that can be enabled and terminated automatically or manually within a predetermined timeframe. A programmatic approach to monitoring payment risk by applying single rule or multi rule profiles gives financial institutions the ability to address specific depositor groups.

More companies are using RDC as a cost saving method of submitting deposits to financial institutions and the pressure is on these institutions to accept deposits directly or, in many cases, by way of a third party. Accepting these deposits introduces unsettling new exception or fraud possibilities to institutions that are not ready to adequately manage the risk. Looking for duplicate items in a customer’s RDC deposit is not adequate to check those that may appear in duplicate files, in checks scanned more than once by the depositor in different deposits or at different locations, by the accidental or intentional reuse of a check or check information for a deposit to another bank, by human error in retrieving a wrong file, and through several other types of fraudulent acts. Therefore, solutions used by financial institutions must provide duplicate item detection across multiple deposit sources. Payments from remote capture must be able to be matched against other payment sources, including POD, branch capture, image exchange, lockbox, ACH, etc.

Another critical requirement for risk mitigation solutions is an operational capability to know when risk policies have been breached and then quickly review, process, and resolve exceptions - preferably before they are posted. Solutions that provide automatic notices, “quarantine areas”, work lists, and supports processing decisions for downstream applications like returns and DDA will be essential to integrating risk assessment, risk management, and policy enforcement. As part of administering the risk solution, alert notices should include automated reminders to review rules and profiles at certain time periods to ensure updates are made to address any changing risk patterns.

The value of a risk mitigation solutions increases if the financial institution can incorporate data-feeds from DDA such as new accounts, closed accounts, inactive accounts, or seasonally inactive accounts. This information can be used to flag suspicious account activity and allows the financial institution to examine and decide whether or not to process the deposit in a pre-post DDA timeframe. Removing identified risk activity from the payment files prevents the added labor costs to reverse the effects of posting. This strategy means that more Day 2 fraud features and functions can be moved to Day 1, enabling the bank to isolate, delete, notify and efficiently handle any suspicious payments hours in advance of current back office handling.

Ideally, risk mitigation solutions should also deliver standard capabilities directly related to risk mitigation. These include monitoring and executing IQA (Image Quality Assessment), duplicate detection as discussed earlier, rebalancing deposits, ensuring MICR integrity, and delivering reports and information that help financial institutions reduce costs and create revenue from these additional services.

Lastly, a comprehensive software solution to address risk should provide audit, operational, and activity reports. To meet audit requirements, banks and aggregators must be able to identify every deposit file, every item, every activity, and every result of the automated and manual risk process for inbound payment files.

The following outline provides the basic list of capabilities required to perform dynamic monitoring and processing of remote captured payment files, as they are received, as part of a comprehensive risk mitigation process:

Capabilities Overview

- Rules based analysis engine
- Extensible business rules that can be grouped into profiles and applied to any relationship level including bank (enterprise), source, customer, and account
- Business rules with configurable thresholds that can test deposit velocity metrics such as frequency, dollar value, item value, etc.
- Exception handling for duplicate items, IQA, closed accounts, etc.
- Workflow for automated exception handling and assignment of quarantined items to work lists
- Notifications and alerts of policy exceptions
- Comprehensive reporting
 - Operational performance metrics (i.e. items quarantined relative to items declined)
 - Monitoring reports
 - Point in time and trend reports
 - “What-if” reports to test or gauge risk potential or effect of new risk rules and profiles
- Ability to process multiple file formats
- Ability to identify and process files from multiple sources
- Provide options for pre-posting intervention and for post posting notices and reports

SUMMARY

In the next 18 months, the financial industry will see an expansion of “self-service deposits” that will speedup the payment process and raise the risk of error and fraud to banks, aggregators, and ultimately their customers. If the risk can be managed and mitigated, the expanded use of RDC promises lower costs and higher customer satisfaction levels. All of these changes are enabled by the push of new technologies that permit bank customers, from consumers and small businesses to larger commercial clients, to capture check images on cell phone cameras, desktop scanners, and even fax machines and to send them to a processor for deposit. Processors may or may not be a financial institution and, in many cases, will be newly formed third party bank-agnostic aggregators of check data and images, capable of sorting them for transmission to a bank of their customer’s choice. In this new world of check processing, banks will be presented electronic deposit files where the entire process has been handled by unknown third parties. To fully engage the FFIEC Guidelines for RDC, banks must be able to analyze each and every deposit and its contents “before posting to DDA”.

The solutions to support the new risk processes require more than duplicate detection and must interject business rules to fully assess the risk potential in every deposit. Banks and aggregators will get the highest value from solutions if they are capable of stopping suspicious items before the DDA or other downstream processes. The reductions of costs related to dealing with rejected items on Day 2 in the back office are expensive in terms of resources, related fees, and most importantly customer satisfaction.

Today, new solutions are available to aid financial institutions that want to exceed compliance with the FFIEC Guidelines using the kind of technology discussed in this paper. These solutions also provide a platform for the bank to reduce costs and increase revenue. The key is for banks and aggregators to immediately define risk management processes; build capability now that allows them to stop known risks; monitor potential risks, and rapidly address new risks; and take advantage of the new risk mitigation technologies to improve financial performance and customer satisfaction.

For more information on a new FFIEC compliant application that mitigates deposit risk that is in operation today, contact Eston Fain at 205-999-0856 and ask about **RiskXP™** from AQ2 Technologies.