Smart Device Deposit Risk Can Be Mitigated!

USING TECHNOLOGY TO MITIGATE RDC RISK

INTRODUCTION

A majority of banks and credit unions are waking up to learn that as of 2012 a significant new product offered by their competitors will be **"Mobile Remote Check Deposit"** (M-RDC). The exciting aspect of this new technology as the method of deposit capture is that the camera of the Smart Device connects to the web from any location! How will this new channel be managed by the financial institutions?

By now all banks and credit unions are aware of the benefits and risks associated with Remote Deposit Capture (RDC). Large merchants and mom and pop businesses alike are ready to implement RDC as their means of deposit. The reason is convenience. Unfortunately most institutions feel the risks associated with allowing the small businesses to join are too risky. The few financial institutions today offering this deposit method typically require the consumer to have multiple relationships with the bank such as a mortgage loan or a credit card where credit risk has been analyzed. So how can we enable the masses to use this new method without requiring a complex relationship?

The answer lies in employing low-cost technology to read the deposit as soon as it is received by the bank and analyze it using a rule-rich process. This will allow the bank and the consumer to be notified of any reason the deposit is determined to be unacceptable all within minutes of its receipt. The other option is the financial institution could accept the risk and enact a fee to accept the deposit.

This technology is being used today by a small number of financial institutions but it has not been released to the mass market due to fear of "how to manage the risks". The complete solution requires several new technologies each playing a part and all operating in tight unison.

TECHNOLOGY COMPONENTS

The first step is an app that can operate on any Smart Device such as the Apple™ iPhone, IPAD, any Android Smart Device, or Win7 Smart Device. The app must be supplied by the individual financial institution to ensure the proper guidelines to the consumer in taking a picture of the check within a strict tolerance of angle/skew, image quality, etc. The consumer must take a picture of both the front and back of the check, showing any endorsements or handwritings.

Next, the app will guide the user in "sending" the check image to a specific electronic location where the bank will retrieve the picture and information that was required. The app should allow the deposit to be directed to either a checking (DDA) or a savings account. Future enhancements of the app could enable the consumer to direct the check to be used as a payment for a specific purpose such as credit card or mortgage loan payment.

Once the check has been captured by the consumer to the phone the image and all information required for the deposit are transmitted to the financial institution. When received, a new type of technology can quickly send an email response indicating receipt of the deposit. This email does not necessarily represent acceptance for deposit – although it could. The financial institution would then process the check using "rules" to determine the acceptability of the deposit.

For example: **Consumer A**'s rules may be only 1 check deposit per day; in which there is a limit of check size not to exceed $500 and no more than $2,000 within a 7 day period, with a limit of no more than $5,000 per month. If any parameter is exceeded the bank could send an email to the consumer asking them to respond to several options:

Option 1 – Press a link in the email to enable the deposit by paying a fee of $xx.00

Option 2 – Press a link in the email to cancel the deposit.

Option 3 – Press a link initiating a call to bank customer service to direct handling of the exception.

Note: No action or response by the consumer within "same day" processing hours should result in the deposit being rejected with an appropriate automated follow-up email.

Consumer B may be managed by a completely separate set of rules. These could be smaller dollar limits or larger amounts but with limits as to the number of checks that can be deposited per day. A small mom & pop business with less than 10 checks a day may find this is a very acceptable method of making deposits, thus avoiding a drive to the branch to leave a night deposit. With a rule-rich analytical engine behind the scenes this can easily limit the number of checks deposited by this customer not to exceed a pre-defined number. Further, the rule engine should be able to validate no duplicates (within a reasonable period ex: 30-45 days) have been presented by this consumer.

Consumer C could be similar to either A or B but with the added dimension of permitting checks less than limits permitted by NACHA (currently $50) to be converted to ACH for clearing by the bank of first deposit, thus lowering the cost to the bank for collection.

RICH FEATURES

Financial Institutions need a solution that allows them to set rules to monitor and enforce the depository risk policies it has made with its customers. This includes tracking the number of daily deposits, deposit amounts per period (days, weeks, or months), item amount limits, item count limits, and other parameters. It should also quickly and easily generate management reports that highlight the exception(s) noted for follow-up and when requested automate decision making. Furthermore, the tools must be sufficiently flexible to match risk monitoring requirements to specific risk threats, relationship cycles, and individual consumers. By aggressively monitoring consumer behavior, the financial institution will be enabled to modify the rules and limits for any consumer. As appropriate, these modifications should be communicated to the consumer.

A risk mitigation solution must be able to differentiate between newly established relationships and current customers. The solution must thereby provide the ability for the financial institution to place rules that expire in a set number of days (ex: 30 days) thus keeping a tight rein on the initial use of the Smart Device for check deposits. It would then automate loosening them if the consumer has not had any negative behavior in the tested time period. A programmatic approach to monitoring

behavior provides the financial institution the ability to address specific depositor groups such as mom & pops vs. individual accounts or even by account type – e.g. savings vs. DDA.

EXPANDABILITY

A financial intuition should be able to expand the M-RDC technology in order to manage other forms of customer self-service deposits such as Remote Deposit Capture (RDC), ATM, Virtual Vault or Lockbox deposits. Expanding across multiple channels should allow some rules and features to become stronger; for example the ability to inspect deposits for duplicates across channels and to better control depositor behavior regardless of the channel of deposit activity.

A critical requirement for risk mitigation is an operational capability to know when risk policies have been breached and to quickly enable review, process actions, send alert emails, and where appropriate automatically resolve exceptions before the deposit is presented for posting. Solutions that provide automatic notices, quarantine areas, work lists, and support processing decisions for downstream applications are essential to integrating risk assessment, risk management, and policy enforcement. Alert notices must include automated reminders to review rules periodically to ensure updates are made to address any changing risk patterns in consumer/customer behavior.

SUMMARY

The value of risk mitigation for check deposits received via Smart Devices increases if the financial institution incorporates within the rules engine a daily data-feed from DDA such as new accounts, inactive accounts, or seasonally inactive accounts. This information can be used to flag suspicious account activity allowing the financial institution to decide whether or not to post a deposit. Removing identified risk activity from the payment files before posting prevents the added labor costs to reverse the effects of posting. This strategy means that some Day 2 fraud functions can be moved to Day 1, enabling the bank to efficiently handle any suspicious payments hours in advance of current back office handling.

Lastly, a comprehensive software solution must provide audit, operational, and activity reports. The financial institutions must be able to identify exceptions for every deposit file, every debit item, and every rule result in a timely manner; all in Day1.

ABOUT

AQ2 Technologies LLC:
AQ2 transforms paper-based payment processes into streamlined digital workflows by seamlessly integrating imaging, data recognition and data management technologies. For more information on a new FFIEC compliant application that mitigates deposit risk that is in operation today, contact Eston Fain, (estonfain@yahoo.com) or sales@aq2tech.com and ask about RiskXP™.