

Agile Risk Management

A Remote Deposit Capture Imperative



Ensentia Corporation
www.ensentia.com

Table of Contents

Executive Summary	4
The Changing Payments Landscape	6
The Argument for Agility	7
Casting a Wide Filtered Net	8
A Day Late, and Dollars Short	10
To Hold From This Day Forward	12
The (Multi-) Level Policy Playing Field	14
Conjoined Twins- Customer Service and Risk	16
Practice Makes Perfect	17
Signed, Sealed, and Delivered	18
False Realities: Both Positive and Negative	19
The Ensenta Difference	20
Contact	21

Executive Summary

The U.S. payments landscape has undergone a major transformation, with the physical transportation of checks replaced by the capture, processing, and clearing of check images from diverse points of deposit, including branches, kiosks, ATMs, merchant locations, homes, and mobile phones. The unprecedented convenience for customers has also ushered in a new set of risks, from outright fraud as well as unintended errors.

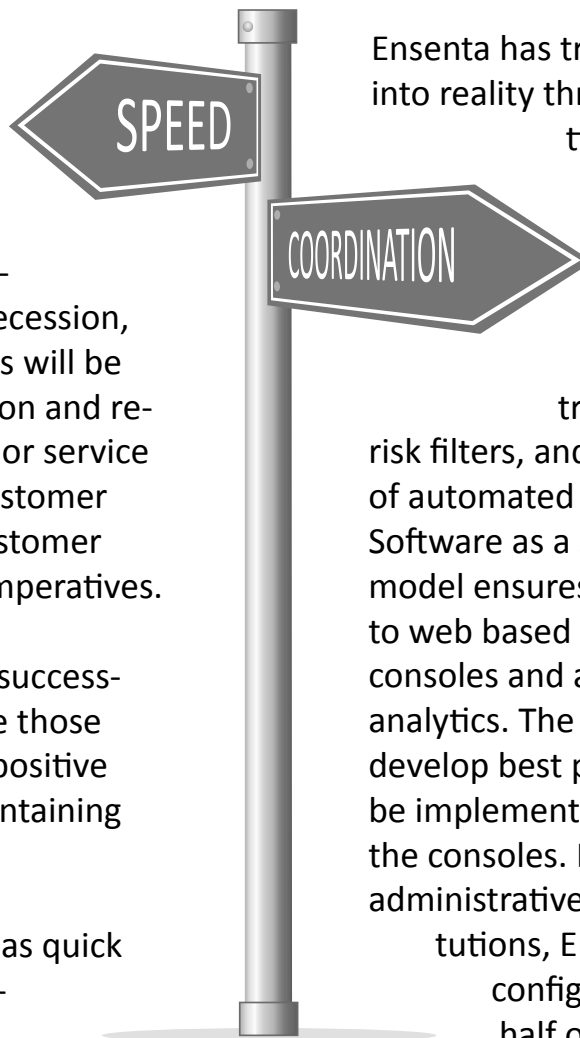
As the financial services industry emerges from the Great Recession, the battle between institutions will be for customer deposit acquisition and retention. The delivery of superior service will be critical in enhancing customer loyalty. Risk mitigation and customer service are often competing imperatives.

In the battle for deposits, the successful financial institutions will be those that can ensure a consistent, positive customer experience while containing deposit risk.

The dictionary defines “agile” as quick and well coordinated in movement. The Ensenta Agile Risk

Management paradigm is based on a careful synthesis of these two attributes- speed and coordination. It combines speed in identifying and mitigating risk, with the coordinated modification of risk management and customer service policy through the continuous development of best practices.

Ensenta has translated the paradigm into reality through the astute combination of an innovative risk engine and a flexible delivery model. The Ensenta Risk Policy Management Engine provides granular control of over 100 real-time risk filters, and the optimal combination of automated and human review. The Software as a Service (SaaS) delivery model ensures secure and easy access to web based risk policy administration consoles and a broad set of real-time analytics. The analytics can be used to develop best practices, which can then be implemented immediately through the consoles. In order to reduce the administrative burden for financial institutions, Ensenta performs the actual configuration changes on behalf of its customers. Thus, the



engine allows financial institutions to work in tandem with Ensenta to move with agility on the loop between the highest levels of policy formulation and the tactical implementation of controls.

The heart of the agile engine is a set of over 100 parameter driven risk filters which examine all checks from all deposit channels in real-time. The filters govern a wide range of criteria, like duplicate detection across all channels, item type, size of deposit, identity of depositor, deposit channel, etc., gleaned from best practices developed over many years of processing transactions for institutions of all sizes. A key aspect of the Ensenta difference is that all filters, administration, and review consoles are accessible in one place. This obviates the need to enter and exit multiple applications, depending on deposit channel or item type.

Unlike conventional batch based systems that review some items for risk on Day Two, the Ensenta system looks at all items at the earliest point in the cycle- Day Zero. Filters have different Severity levels for On Us and Guest (Transit) items, which drive the Hold Period and review modality. The Severity levels can be set through the administration consoles at default levels, by each deposit channel or customized based on financial institution policy,

thus providing institutions significant flexibility in aligning tactical policy implementation with their risk management strategy.

To effect the strategic intersection between risk management and customer service, the engine can also do the opposite and provide accelerated funds availability to selected customers, account types, or specific check types. These hold overrides allow financial institutions to offer the winning balance between a consistent, positive customer experience and risk containment.

A rich set of real-time analytics, available securely over the web, enables financial institutions to gain insight into their transactions, including trends in false positives and negatives. This capability completes the feedback loop between best practice, policy formulation, and implementation of controls.

In a rapidly evolving competitive landscape, financial institutions need to include agility as a competitive differentiator in translating strategy to action. They need to balance service delivery and risk management in a winning combination.

Agile Risk Management offers an attractive way forward.

The Changing Payments Landscape

Recent years have seen the dramatic transformation of the U.S. check payment infrastructure. The transportation and processing of paper at the many labor intensive facilities across the nation has given way to the electronic capture, validation, and clearing of check images. With improvements in scanning, recognition, and image transmission technologies, the point of image deposit capture has radiated outward from financial institution branches to include ATMs, check scanners at businesses, flatbed scanners in homes, and even mobile phones. Though the transformation has resulted in tremendous efficiency gains for financial institutions, and unprecedented convenience for consumers and businesses, it has also ushered in a new set of risks.

An obvious source of risk in this brave new world is fraud by technology savvy criminals. According to the American Bankers Association Deposit Fraud Survey Report of 2009, annual industry losses from check fraud are estimated at \$1.024 billion. Perhaps not so

apparent are unintended errors by customers or financial institutions dealing with unfamiliar systems. The compliance requirement driven by a quickly evolving regulatory regime adds another dimension to the risk challenge. While it is tempting to address risk by batten- ing down all hatches, it is important to carefully consider the impact on customer satisfaction.



As the banking industry emerges from the challenges of the Great Recession, the contest between institutions will be to acquire and retain deposits. It is clear that service delivery will be critical in enhancing customer loyalty. According to Bain and Company¹, the most loyal bank customers cited “service” over six times more frequently than “rates and fees” or “branches”, as their top reason for recommending their bank to others.

In the battle for deposits, the successful financial institutions will be those that can ensure a consistent, positive customer experience while mitigating deposit risk.

¹Customer loyalty in retail banking: North America 2010, Bain and Company Financial Services Practice

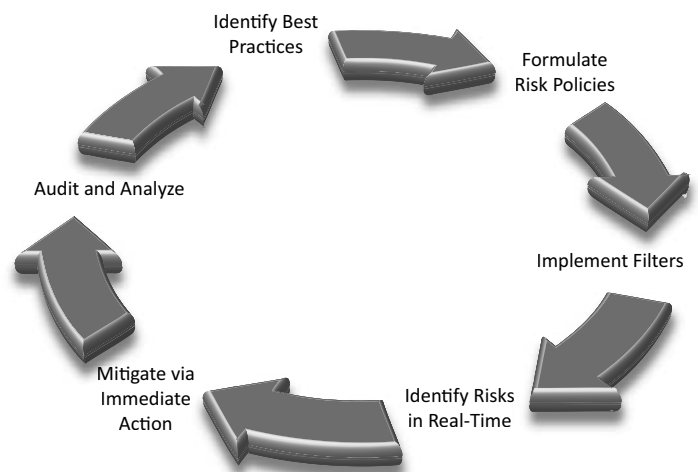
The Argument for Agility

The dictionary defines “agile” as quick and well coordinated in movement. The Ensenta Agile Risk Management paradigm is based on a careful synthesis of these two attributes- **speed** and **coordination**.

The need for speed is driven by the instantaneous nature of electronic transaction processing, customer expectations shaped by experience on other real-time media like the Web and mobile telephony, and the rapid introduction of new financial services (primarily from non-financial competitors).

Speed for its own sake, however, only addresses a piece of the puzzle. There is also the need to coordinate customer acquisition and retention strategy, enterprise risk policy, best practices, analysis, regulatory compliance, system security, and usability.

The case can thus be made for a real-time enterprise risk policy management engine that allows financial institutions to go swiftly from policy formulation to implementing parameter driven filters for all deposit channels and across varied customer segments. The system should also provide best practices feedback to allow institutions to continuously improve their policy regimes.



The combination of policy coordination and speed shown in Figure 1 requires the following attributes:

- Comprehensive set of parameter based, tunable risk filters
- Risk identification and action at the earliest point in the payments processing cycle
- Multiple real-time risk review and mitigation options
- Policy administration at default, channel, and institution levels
- Flexible override capability
- Extensive risk analysis and reporting
- Nimble and secure service delivery infrastructure

Casting a Wide Filtered Net

The heart of a risk management system is a comprehensive set of filters that can identify risks in real-time. The filters are driven by the best practices that stem from monitoring all items that pass through a transaction processing system- the broader the transaction processing ecosystem, the better the continuous improvement. The Ensenta system is built on the many years of learning from processing check deposits for banks and credit unions of all sizes, and across all points of deposit, including branches, ATMs, kiosks, merchant locations, homes, and mobile phones.

The Ensenta Agile Risk Policy Management Engine has over 100 parameter tunable, real-time risk filters that examine a wide range of potential risks. These filters are driven by best practices gleaned from several years of

processing transactions for financial institutions of all sizes. Some examples include duplicate detection across all items and all deposit channels (and multiple participating institutions) for one year, black listed routing numbers, amount thresholds, and various factors that ensure integrity of the check and the account.

Also included are Image Quality and Usability filters that address the Financial Services Technology Consortium (FSTC) Image Defect Metrics. The metrics are parameter driven, and can be customized to fit individual financial institution criteria.

Filters have assignable three-level Severity ratings that drive mitigation action. The Severity rating can be set separately for On Us

Risk Filter	Transit Severity	On-Us Severity	Depositor Confirm	OCR Required
Filter 1	1, 2 or 3	1, 2 or 3	Y/N	Y/N
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
x	x	x	x	x
Filter 100+	1, 2 or 3	1, 2 or 3	Y/N	Y/N

Figure 2 - Risk Filter Administrative Options

and Guest (Transit items). Where applicable, the system has the option of requesting confirmation by the depositor (in the case of merchant, consumer, and mobile deposits), and/or using Optical Character Recognition (OCR) to determine an item risk confidence level. Getting confirmation by the depositor can help eliminate errors at the earliest point in the deposit stream, thus reducing costly error correction later in the cycle.

In order to preserve the agility that is the cornerstone of this approach, it is absolutely essential that the administration of the various

filters is convenient. Anything more complex will negate the very basis of the system. A key strategic difference in the Ensenta approach is that all filters, administration, and review consoles are accessible in one place. This obviates the need to enter and exit multiple applications, depending on deposit channel or item type, and provides users a concise, self-contained, and actionable perspective on risk.

An example of the Ensenta administration console is shown in Figure 3 below.

EZAdmin Deposit Policies

View/Edit
Print/Export

Institution
Ecotopia FI - My Deposit

Description
Ecotopia FI Default

Standard Hold
Local

Extended Hold
Local

Annotation Code
None

Default?
Yes

Still Valid?
Yes

Threshold	Value	Associated Risk
Check Amount Threshold (High)	0.00	Too High Amount
Check Amount Threshold (Medium)	0.00	Large Amount
Check Amount Threshold (Low)	0.00	Lower Amount
OCR/Customer Amount Variance Threshold (High)	5000.00	Amount Variance Exceeds Threshold
OCR/Customer Amount Variance Threshold (Medium)	10.00	Amount Variance Exceeds Warn Value
OCR/Customer Amount Variance Threshold (Low)	0.00	Amount Variance Exceeds Low Warn Value
Risk Score Threshold (High)	0	Exceeds High Score
Risk Score Threshold (Medium)	0	Exceeds Medium Score
Risk Score Threshold (Low)	0	Exceeds Low Score

Deposit Policy Risk Factors

Deposit Risk Factor	Deposit Risk Severity
Amount Not Recognized By OCR or Overridden	Reject
Amount Variance Exceeds Low Warn Value	Std Hold - Flag
Amount Variance Exceeds Threshold	Std Hold - Flag
Amount Variance Exceeds Warn Value	Std Hold - Flag
AuxOnUs Length Invalid	Std Hold - Flag
AuxOnUs Value Invalid	Std Hold - Flag
Back Image Too Light	Std Hold - Flag
Back Signature Not Detected	Reject
Date Not Recognized By OCR	Std Hold - Flag
Duplicate Code Line	Std Hold - Flag
EPC Length Invalid	Std Hold - Flag
EPC Value Invalid	Std Hold - Flag
Large Amount	Reject
No Routing/Transit Number Found in Codeline	Reject
One or more MICR codes unreadable	Std Hold - Flag
OnUs Length Invalid	Std Hold - Flag
OnUs Value Invalid	Std Hold - Flag
Routing Digit, Length, Branch, or Series Invalid	Reject
Routing Number Check Digit Incorrect	Reject
Savings Bond	Std Hold - Flag
Too High Amount	Std Hold - Flag

Action for selected ID: New Entry

<< Please Select Action >>

Figure 3 - Risk Filter Administration Console

A Day Late, and Dollars Short

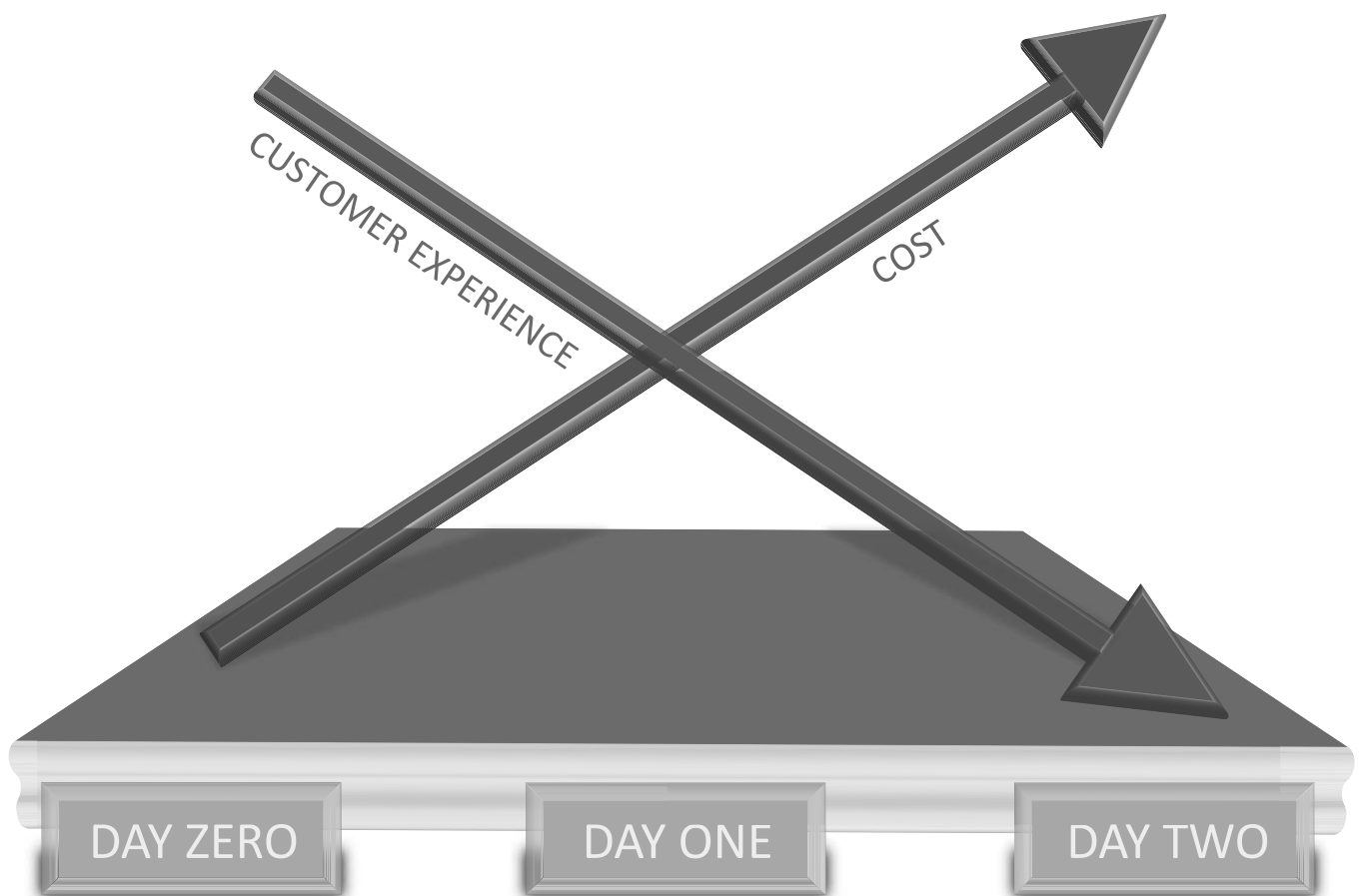


Figure 4 - Impact of risk mitigation at various points on the payments life cycle

Agility means not only *how quick*, but also *when* an action is taken.

The traditional check processing workflow calls for some level of error checking on Day One, and examining selected items for potential fraud on Day Two or beyond- Day

One being the day of item capture, and Day Two the next day. This is a holdover from the paper processing days, when it took time for physical paper to move from the branch to a central processing center for clearing. Even though the industry has moved on to electronic images, most risk management systems

follow a batched workflow on Day Two- essentially an automated version of the old paper process.

With distributed deposit capture and the electronic clearing and exchange of check images, the old Day One and Day Two have telescoped into “Day Zero”. Both deliberate fraud and unintended errors can proliferate at electronic speed. Because of the number of elapsed steps in the workflow that may have to be reversed, waiting for later in the check

processing life cycle to address risk increases cost. Similarly, the impact on the customer experience is likely to be more negative later in the life cycle. Clearly, a system that identifies risk and takes action to at the earliest Day Zero opportunity makes eminent sense.

The Ensenta Agile Risk Policy Management Engine follows the Do It Right The First Time (DRIFT) principle in processing all items across all deposit channels at the Day Zero point of entry into the payment processing stream.

To Hold From This Day Forward

The main avenue of risk containment action is to hold checks and subject them to manual review. The Hold Period is dictated by the Severity rating assigned to the specific filter. The Hold Periods corresponding to the Severity ratings are as follows:

- Standard Hold
- Extended Hold
- Rejection (for Merchant, Consumer, Mobile) or FI Review (for all other channels)

If a check trips multiple filters, the Hold Period will be based on the highest Severity rating. The actual Hold Periods can be set based on individual financial institution policy.

In addition to the Hold Periods, the system can request the depositor to review a deposit. In cases where there is a discrepancy between the Depositor Review and OCR, the check is automatically routed for review by financial institution personnel. Some examples of Depositor Review include missing endorsements, date verification (stale, post-dated, missing), missing signature, amount discrepancy, etc.. It must be noted that Depositor Review is not the same as Rejection. While Depositor Review leverages the depositor to correct discrepancies, and thus reduce the workload for the financial institution, a Rejec-

tion blocks a check from entering the payment stream. In the case of branch and ATM deposits, since the depositor is not present, checks that qualify for “Rejection” are directly sent to financial institution personnel for review.

Thus, the Ensenta system offers an optimal blend of automated and human review with complementary layers of examination:

- Automated filters
- Depositor review
- Financial institution review

The system also facilitates the Know Your Customer (KYC) requirement faced by financial institutions by maintaining lists of Excluded and Included customers for merchant, consumer, and mobile deposits. These lists are usually based on account history or other types of financial institution due diligence. Through Single Sign On, access to these remote deposit applications can easily be controlled. In the event an account appears on both Excluded and Included lists, the Excluded list takes precedence to ensure proper risk control.

Financial institution review is made possible by grouping checks into two queues:

- **Need Review Queue-** Certain risk filters can be set to examine whether checks require further review. Checks that trip these filters are routed to a Needs Review Queue. All items in the Needs Review Queue have to be reviewed by the financial institution.
- **One Click Approve Queue-** All items that did not trip any risk filters can be approved for inclusion in an Image Cash Letter (ICL). A drill down capability allows reviewers to check item details if necessary.

During the review process, the item can be

corrected or returned with one of more than 25 appropriate reason codes. The Ensenta Agile Risk Policy Management Engine can be integrated with financial institution returns processing systems. Examples of return reason codes include Not Sufficient Funds (NSF), Uncollected Funds (UCF), Stop Payment, Missing Signature, Altered/ Fictitious Item, etc. All review, editing and return can only be performed by authorized personnel. This is controlled by a robust role-based authentication capability. Items that pass review are moved to the Reviewed Queue for inclusion in the next ICL.

An example of review and item drill down is shown in Figure 5.

EZAdmin Check21 Express

Search Institution Selection: All Available Institutions Exclude Branch Capture?: Yes Mask Acct Number: Yes

Check21 File	Cutoff Date/Time	Generation Date/Time	Branches	Held Queue	Need Review Queue	One Click Approve Queue	Approve Now	Reviewed List	Auto Approved List	Return List	All Items List
All			All		30	115	<input type="button" value="Approve"/>	1			145
Ecotopia FI My Deposit	02/11/2011 15:00	02/11/2011 15:30	Ecotopia FI My Deposit 97067		1		<input type="button" value="Approve"/>				1

EZAdmin Check21 Express

Click OK to approve, Adjust to change, or Back to Summary

File: Ecotopia FI My Deposit File Status: Yes Cutoff: 02/11/2011 15:00 Institution: All Available Institutions Queue/List: Needs Review Branch: All

Transaction Date/Time: 02/10/2011 15:33
 Check21 File Generated: Not yet generated
 Account: x2=15
 Transaction Type: Deposit
 Station: Ecotopia FI My Deposit 97067
 Acquirer / Issuer: Ecotopia FI / Ecotopia FI
 OCR Amount: \$9.00
 Customer-Entered Amount: \$9.00
 Deposit Type: Not Applicable / Other

Risk Factor(s): Date Not Recognized By OCR

First Party Payee(s): LEFTY GROVE, Ecotopia FI

Aux On-Us	EPC	Routing/Transit	On-Us	Amount
999006		121143260	833222444V	9.00

In the Aux On-Us & On-Us fields, use V for the On-Us symbol and - for the dash symbol.
 To accept: select new status & click "OK Next". To adjust: make changes & click Adjust.

Current Review Status: Needs Review New Review Status: Review Complete

<< Back to Summary Adjust OK Next >>

Figure 5 - Item Review and Drill Down Capability

The (Multi-) Level Policy Playing Field

Financial institutions set risk policy based on competitive strategy and threat assessments. These assessments can assign varied risk levels to the different available deposit channels. For example, the risk associated with channels emanating from outside a financial institution’s physical infrastructure (like merchant locations, homes, and mobile phones) can be different from branch and ATM deposits. Thus, risk policy has to be viewed at multiple levels, including:

- System or default level
- Deposit Channel level
- Financial institution level

At the System level, risk profiles such as filter Severity levels, thresholds, Hold Periods and review modalities are pre-set based on practices frequently used by the many financial institutions using a Software as a Service (SaaS) network, such as Ensenta.

View/Edit
Print/Export

Institution
Ecotopia FI - My Deposit

Description

Standard Hold

Extended Hold

Annotation Code

Default?

Still Valid?

Threshold	Value	Associated Risk
Check Amount Threshold (High)	<input type="text" value="0.00"/>	Too High Amount
Check Amount Threshold (Medium)	<input type="text" value="0.00"/>	Large Amount
Check Amount Threshold (Low)	<input type="text" value="0.00"/>	Lower Amount
OCR/Customer Amount Variance Threshold (High)	<input type="text" value="5000.00"/>	Amount Variance Exceeds Threshold
OCR/Customer Amount Variance Threshold (Medium)	<input type="text" value="10.00"/>	Amount Variance Exceeds Warn Value
OCR/Customer Amount Variance Threshold (Low)	<input type="text" value="0.00"/>	Amount Variance Exceeds Low Warn Value

Figure 6 - Risk Policy Level Administration

The Deposit Channel level allows the setting of risk profiles unique to each deposit channel (like branch, merchant etc.). In addition to the obvious benefits of protecting an institution from loss, this has the added benefit of aiding compliance with regulations and guidelines like the Federal Financial Institution Examination Council (FFIEC) issued Risk Management of Remote Deposit Capture. Deposit Channel criteria supersede the System level presets.

The pinnacle in the risk policy hierarchy is the Financial Institution level, where policies for a specific financial institution can be set. These override Deposit Channel and System level

settings. This capability allows an institution to actualize the agile risk policy management paradigm shown in Figure 6.

In the Ensenta SaaS environment, the ability to modify risk profiles at the granular levels discussed is strictly controlled through a role-based credential authentication system. This ensures the alignment and stability of implemented filters with financial institution policy.

Conjoined Twins- Customer Service and Risk

EZAdmin Depositor Classes

The screenshot shows the EZAdmin interface for managing Depositor Classes. It includes a top navigation bar with 'View/Edit' and 'Print/Export' buttons. The main content area is divided into several sections:

- Account Details:** Institution (Ecotopia FI - My Deposit), Description (Ecotopia FI Hold Override), Account Holder Number (input field), Account Holder Group (Not Applicable / Other), and Remote Deposit Policy (Not Applicable / Other - Ensenta Corporation).
- Guest?:** No
- New Account?:** No
- New User?:** No
- Default?:** No
- Still Valid?:** Yes
- Deposit Policy Assign:** A table showing the assignment of a deposit policy to an institution and depositor class.
- Deposit Limits:** A table defining limits for deposit policies across institutions, including deposit limit periods, depositor classes, maximum transaction amounts, and maximum amounts.

Deposit Policy	Institution	Depositor Class	Valid?	Id
Ecotopia FI Default	Ecotopia FI - My Deposit	Ecotopia FI Hold Override	Y	74

Deposit Policy Limit	Institution	Deposit Limit Period	Depositor Class	Maximum Transaction	Maximum Amount
----------------------	-------------	----------------------	-----------------	---------------------	----------------

Figure 7 - Hold Override Management

The need to maintain a positive customer experience is often overlooked when managing risk. As discussed earlier, maintaining customer loyalty is critical in the ongoing war between institutions for deposits. Thus, instead of extending holds based on flagged risk filters, it may be necessary to do just the opposite and accelerate funds availability for carefully identified groups of customers, or types of items.

For example, savvy customer retention strategies will identify premium customers for accelerated funds availability, regardless of risk filters. Similarly, accelerated availability, regardless of risk filters, can be given to payroll or expense reimbursement checks. Hold overrides can also be made depending on the account type. For example, it may be desir-

able to expedite funds into payer accounts like loan accounts.

Therefore, a smart risk management system needs to have overrides based on criteria such as:

- Depositor profile
- Check amount
- Account type
- Check type (payroll or company expense checks)

The Ensenta Agile Risk Policy Management Engine allows financial institutions to fashion a win-win strategy that successfully addresses both customer retention imperatives and real-time risk avoidance.

Practice Makes Perfect

The ability to continuously refine risk management policy based on best practices is predicated on the ability to observe and analyze the many granular dimensions discussed in this paper. Thus, a flexible reporting and analysis capability that renders relevant information to financial institution is required. There are three aspects to be considered in a best practices driven environment:

- Breadth of readily available analyses
- Timeliness of underlying information
- Ease of access

An agile system must have the ability to conduct analyses and present insights to financial institution users. It is not enough to make raw data available, as this places the burden of

analysis on the user.

The analyses need to be based on the most current information available. In the electronic world, risk moves at the speed of light, and so should mitigation.

The insight should be readily accessible. The very notion of agility is defeated if users have to go through multiple steps to access and export analysis.

The Ensenta Agile Risk Policy Management Engine provides a broad array of real-time, web delivered analytics to help financial institutions hone best practices and refine policy. Figure 8 shows an example of some of the available analyses.

EZAdmin Reject Analysis

Start Date/Time:
End Date/Time:
Station:
» Clear All Selections

All Items: 550 Includes Rejected Items, Cancelled Items, and Successful Deposits/Payments
Correct/Retry Successful if successful deposit/payment within 10 minutes of initial cancel/reject for same account holder at same station
Duplicate if identical error within 2 minutes of initial cancel/reject for same account holder at same station. Duplicates considered a single item.
Failed if no successful deposit/payment within 10 minutes of initial cancel/reject for same account holder at same station

	Reject/Cancel Reason	Deposit/ Payment Items	% All Rejects	Deposit/ Payment Amount	Successful After Correct/Retry	% Successful After Correct/Retry	Failed Items	% All Items	Failed Despite Retry	% All Items	Abandoned Without Retry
» Show Detail	13 - Invalid amount	1	1%	\$2,981.11	0	0%	1	0%	0	0%	1
» Show Detail	55 - Incorrect PIN	4	2%	\$3,182.55	1	25%	3	1%	1	0%	2
» Show Detail	57 - Transaction not permitted to cardholder	1	1%	\$2,000.00	0	0%	1	0%	0	0%	1
» Show Detail	Cancelled by account holder	6	4%	\$0.00	0	0%	6	1%	1	0%	5
» Show Detail	Cancelled by account holder (reviewing risk 'BadPayeeName')	3	2%	\$496.00	2	67%	1	0%	0	0%	1
» Show Detail	Cancelled by account holder (reviewing risk 'NoDate')	2	1%	\$13,581.02	0	0%	2	0%	0	0%	2
» Show Detail	Cancelled by account holder (reviewing risk 'NoSigBack')	7	4%	\$20,470.11	6	86%	1	0%	0	0%	1

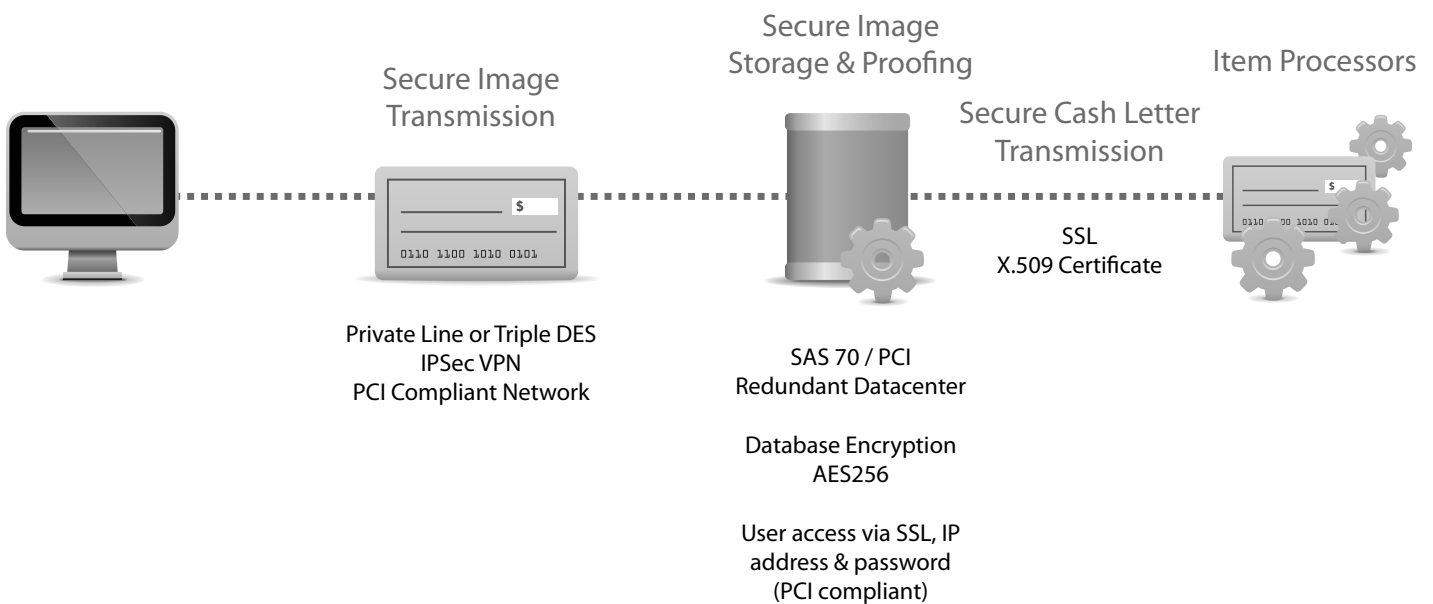
Figure 8 - Reject Analysis

Signed, Sealed, and Delivered

The agility of a system is highly dependent on the delivery model. In spite of the flexible capabilities described in this paper, if making modifications to the system is based on complex implementation processes, a mounting backlog of requirements is bound to swamp the ability of a financial institution to respond nimbly to observed risk patterns, competition, regulation, and technology. In addition to being fast, the delivery model must be safe. After all, the movement of money is about as mission-critical as it gets.

- Software as a Service (SaaS) allows rapid development and implementation of changing requirements
- SAS 70 certification and PCI compliance ensures robust security
- Single Sign On and role based access assures system access only to authorized personnel
- Redundant data centers enhance business continuity

The Ensenta delivery model lends itself well to the need for secure agility:



False Realities: Both Positive and Negative

While discussing risk management, it is important to consider false positives and negatives. While the first unduly flags checks as risky, the second allows risky items to go through. Both are results of imperfect technologies (like character recognition) and human error, which are realities of transaction processing. It is also important to reiterate that the goal is a winning balance between risk management and customer service. Thus, a draconian risk regime that delivers poor service is a non-starter.

While false positives and negatives cannot be completely eliminated, the following capabilities available in the Ensentia system offer avenues to fashion best practices to contain them:

- Multiple review layers-automated, depositor, financial institution
- Extensive real-time analytics
- Over 100 parameter

based tunable risk filters

- Web based risk policy administration consoles
- The combination of the above to identify false patterns and quickly update the system to contain the effects.



The Ensenta Difference

It is clear that the rapidly evolving payments landscape requires a winning balance between risk management and customer service. The Ensenta approach begins with an overarching agile paradigm that combines effective real-time tactical risk controls, with the development of best practices to drive risk policy at the highest strategic levels of a financial institution. Ensenta has translated this paradigm to reality with the astute combination of an innovative system and a flexible delivery model. The multi-layered system offers granular tunability of risk filters, which operate in real-time and across all deposit channels, with an optimal blend of automated and human review. The self-contained filters and consoles give financial institutions a concise and actionable perspective on risk. The SaaS delivery model allows secure, easy access to complete the feedback loop between risk management and customer service policy, and risk mitigation driven through

best practices.

Call us to find out how Ensenta Agile Risk Policy Management can help your financial institution win by ensuring a consistent and positive customer experience while mitigating deposit risk.

Contact

Jim Ballagh
Vice President, Business Development

E-Mail: jim@ensenta.com

Phone: 650-288-1131

Web: www.ensenta.com

Ensenta Corporation
www.ensenta.com