Demystifying Risk Associated with Mobile RDC

Why Read This Report

According to a recent RemoteDepositCapture.com survey, virtually all financial institutions (FIs) will offer mobile remote deposit capture (mobile RDC) within the next year.

This report provides FIs with an opportunity to benchmark against a variety of industry practices and experiences with mobile RDC. A key focus here is in understanding the level and types of risks. As with any channel, the mobile channel has its own set of advantages and risks. Our goal is to help FIs develop a fact base and recommendations that can be used in assessing the risk-reward trade-offs. The findings of this survey will help FIs identify those trade-offs in a way that maximizes their ability to balance the benefits of mobile RDC, independent of their risk appetite.

Key Findings:

- 80% of financial institutions that offer mobile RDC report no losses
- 90% say the benefits of mobile RDC outweigh risks and costs
- 61% of institutions offer customized deposit limits based on policy rules, segmentation, scores and other types of decision analytics
- Many risk management best practices are not widely adopted (e.g. duplicate detection, mobile authentication and modeling of account abuse leading indicators)
- Mobile RDC has reached a critical mass of availability to consumers but is not yet broadly accessible to small businesses and commercial clients.

FIs have an opportunity to deploy risk management best practices while losses are low to get ahead of any emerging risks. This, in turn, will enable them to **isolate risky transactions** and **increase access to low risk and under-penetrated segments** of their portfolio.

Report sponsored by:

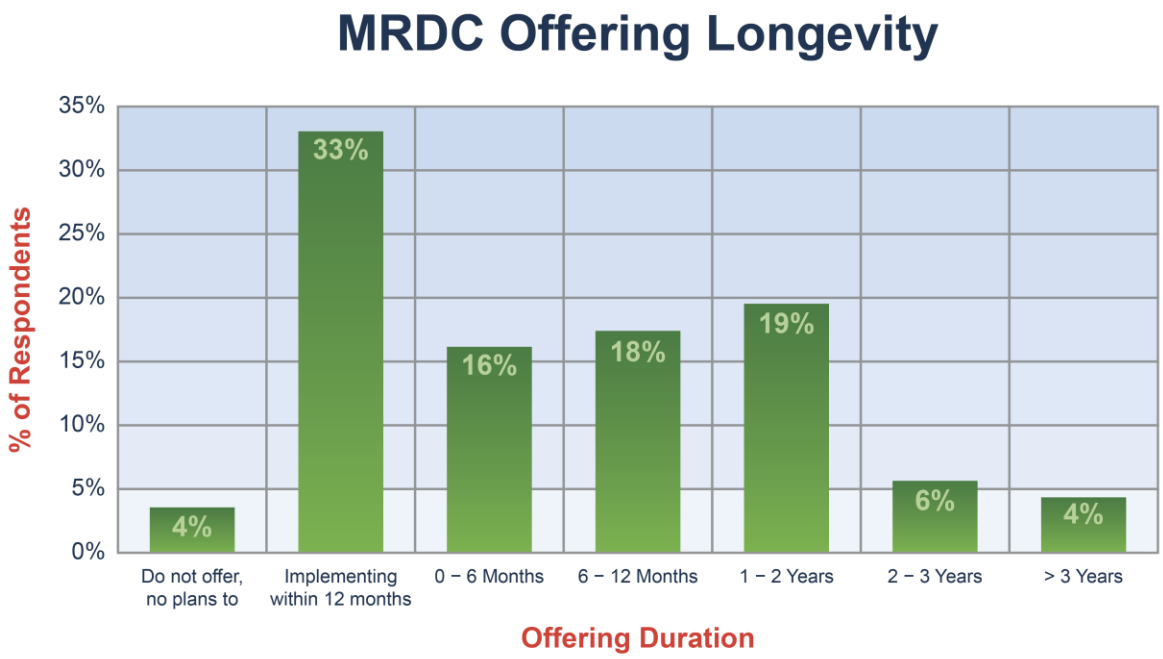
Intelligent Mobile Imaging
Mitek

Methodology

Data measuring the usage, risk management practices, losses and perceived value was collected by RemoteDepositCapture.com survey between February 27th and April 15th, 2014. Two-hundred and forty-six respondents, from a wide cross section of banks, credit unions and brokerages completed the survey.

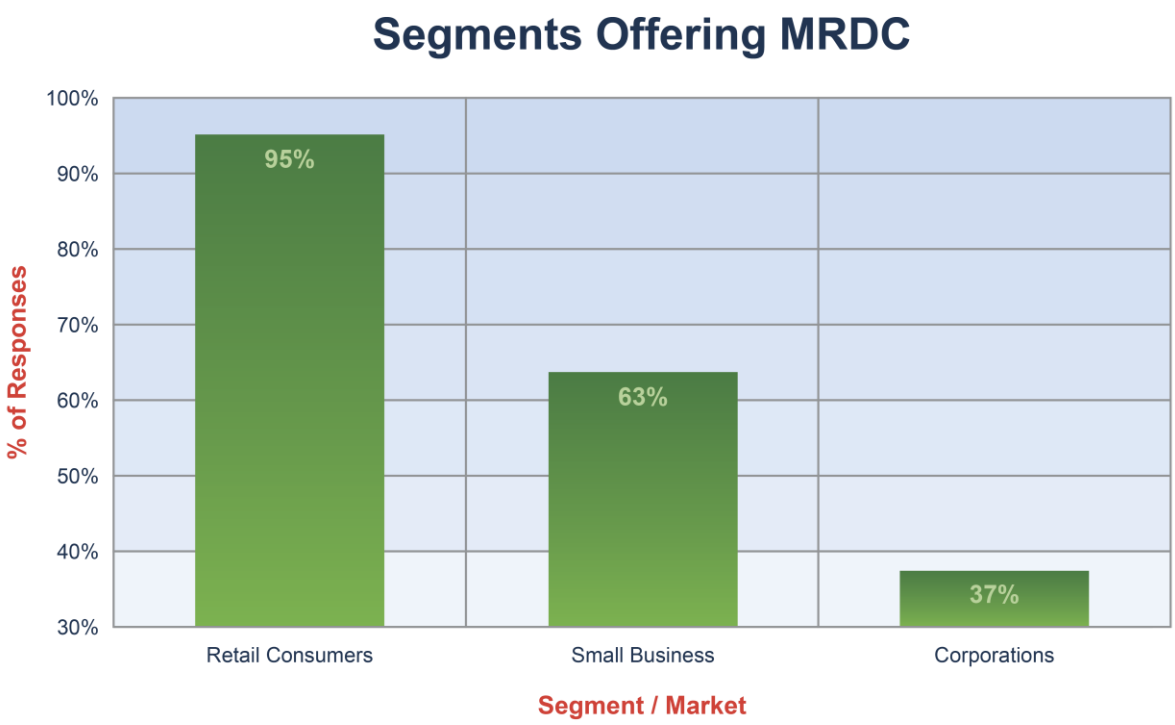
Summary of Findings

Majority of FIs offer mobile RDC and plan to expand to new markets. Sixty-three percent of respondents currently offer mobile RDC and 33% plan to offer it in the next 12 months. Only 4% have no plans for mobile RDC. Perceived value of mobile RDC is highly correlated with experience—**the longer a FI has offered Mobile RDC the greater the perceived value**.



Among those who provide mobile RDC, the vast majority (95%) offer it to their retail clients but only 63% provide it to their small business customers and 37% to commercial customers.

Mobile RDC has reached a critical mass of availability to consumers but is not yet broadly accessible to small businesses and commercial clients.

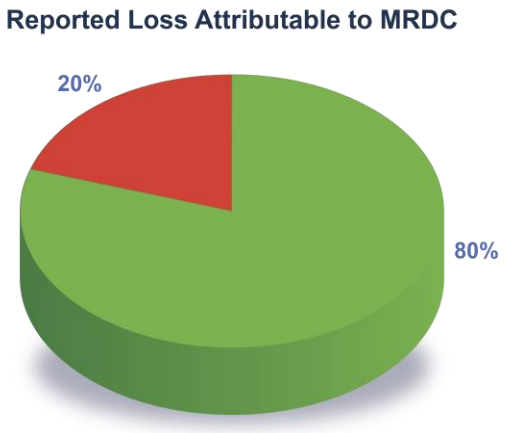


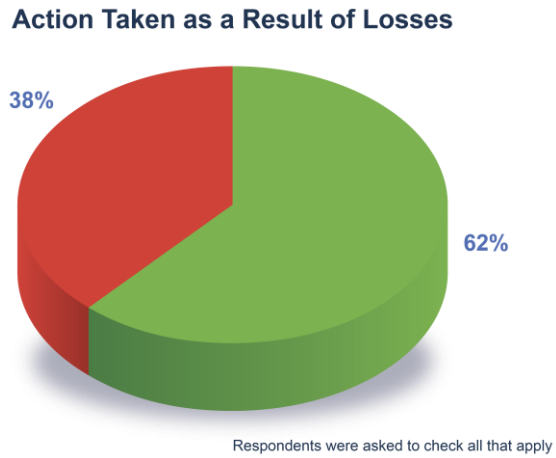
The survey reports that 80% of financial institutions reported no mobile RDC losses. Of those who did report losses, 96% experienced losses from consumer deposits, 15% from small business deposits and none reported losses from corporate mobile RDC deposits.

To be sure, there are risks to be mindful of; each channel has its own set of advantages and risks. The mobile channel brings some added layers of security (e.g. app login, mobile authentication, device insight and location). At the same time, mobile RDC presents new risks and operational processes, principally relating to duplicate deposits – and a growing number of tools available to address those challenges.

And of course, some age old types of fraud compromise (e.g., counterfeits, check washing, account take over, social engineering) can be attempted in any channel.

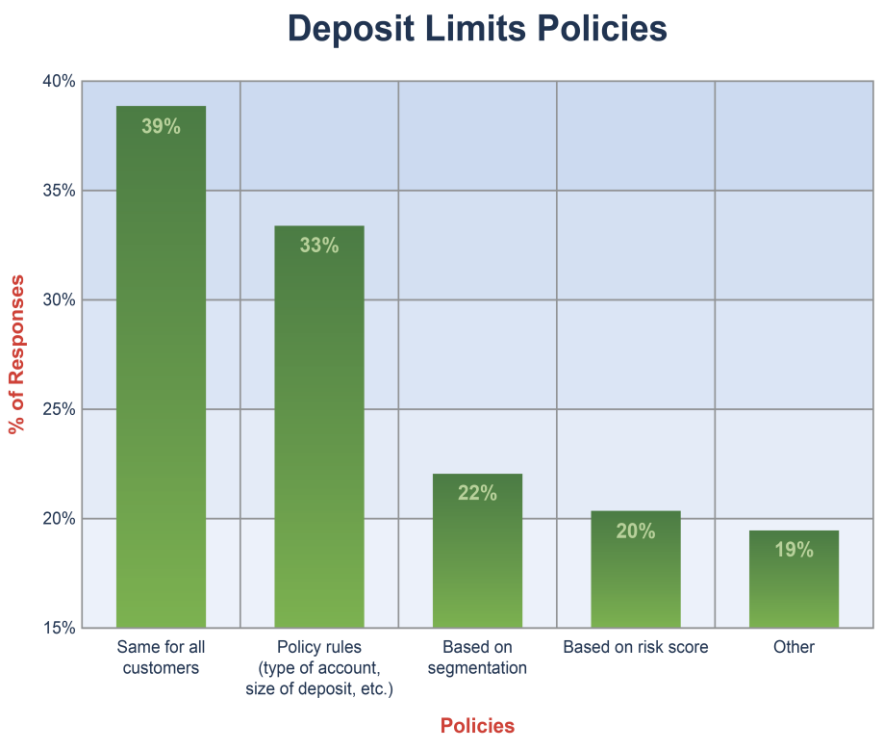
That said, among those 20% that incurred a loss, **62% of FIs who offer the service believe that losses are within their acceptable limits**, and took no action.

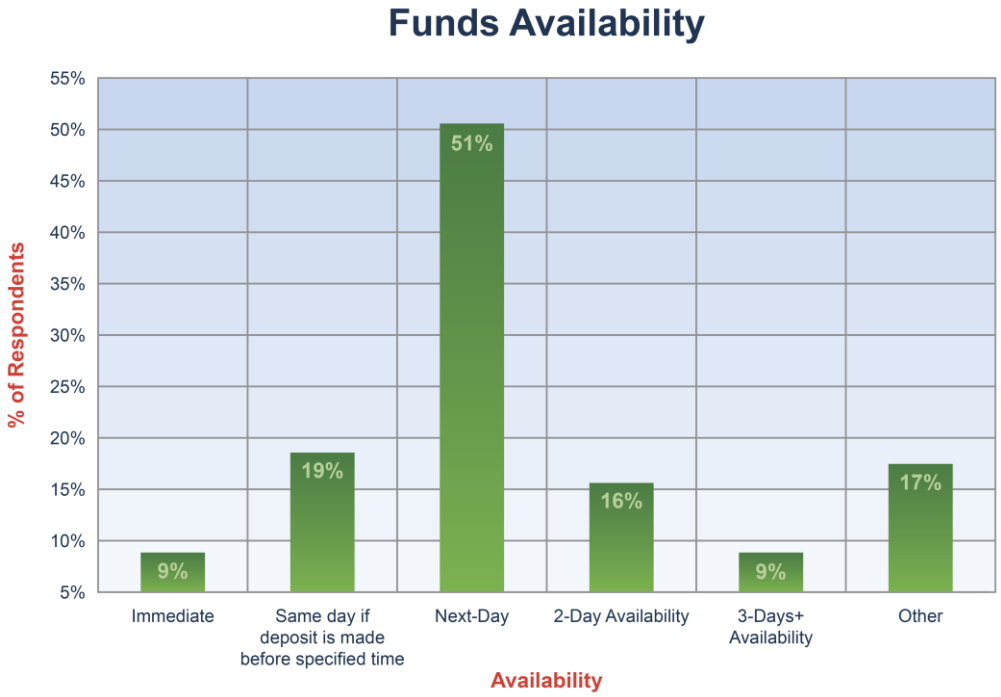




Majority of FIs use custom limits. 61% of respondents are using policy rules, segmentation and risk score for setting custom deposit limits. Thirty-nine percent apply the same deposit limits for all customers. This suggests an opportunity to further refine strategies and tailor "smart limits" to each unique customer segment and profile.

For example, some FIs have indicated that a majority of losses occur with new accounts and have consequently imposed tighter limits on young accounts and more relaxed restrictions on more tenured customers. Other attributes such as risk score, balance and type of account have been proven effective in establishing segmentation schema.





Majority of FIs make funds available the same or next-day. Fifty-one percent of FIs offer next day availability while 28% offer immediate or same day access to funds. A smaller percent of FIs make funds available in days following the deposit, 16%, offer two day availability and 9% offer three day.

Risk management processes and tools vary. There is considerable variability in the types of risk mitigation strategies used by FIs. The majority apply deposit value limits (84%), image quality analytics (IQA)-(71%), CAR/LAR mismatch (59%) and deposit volume limits (54%).

However, there are other techniques that are surprisingly underutilized.

For example, **despite concerns about duplicate deposits, only 49% use cross channel duplicate detection**. Endorsement detection is used by 47% of institutions. Forty-three percent use delayed availability.

Risk management tools inherent to the mobile channel also appear under-utilized. For example, device ID is used by 25% and geo location by 13%. The good news is that FIs have an opportunity to deploy these best practices while losses are still low to maintain the security of the channel.

We expect that, increased **precision in identifying and isolating risky transactions** will **enable FIs to increase access for the vast majority of low risk customers**.

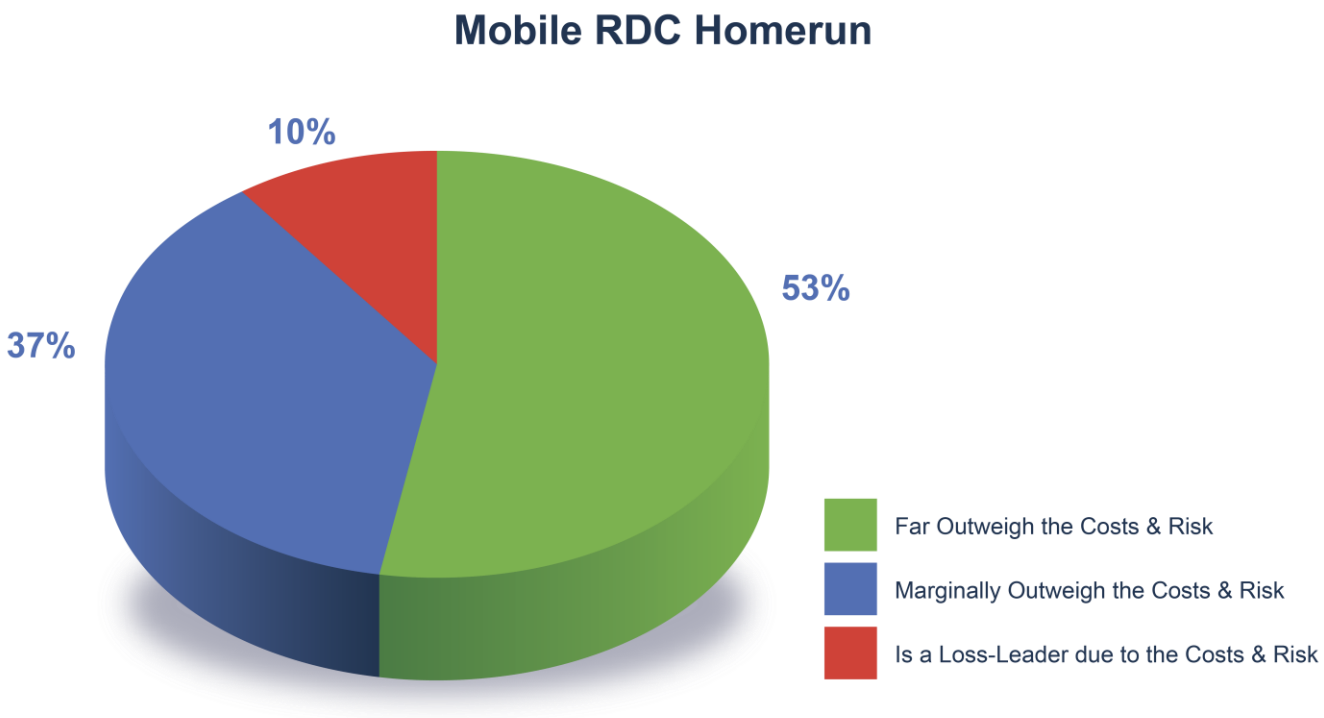
About Duplicates:

Risk managers indicate that the vast majority of duplicates are “accidental duplicates.” To be sure, these accidental duplicates create operational costs and challenges; however, these costs are much lower than the economic impact of a fraud loss or even the opportunity cost of not offering the mobile RDC service.

Among the comparatively smaller population of fraudulent duplicate deposits, the majority tend to be cases of first party fraud in which the actual consumer is engaging in account abuse activity or “testing” the system. This can lead to a gray area and challenges for banks’ ability to classify, track, report and respond to these trends.

Fortunately, there are tools available to these FIs to model leading indicators of account abuse and to better utilize a variety of risk management and analytic tools.

Majority of FIs believe that benefits of mobile RDC far outweigh the costs and risk. Fifty-three percent of respondents believe that the benefits of mobile RDC far outweigh the costs and risks, and 37% indicated that benefits marginally outweigh the cost and risks.



Conclusion

Risk managers are rightfully proud for having protected their financial institution (FI) as well as the consumers they serve. However, imprecise risk controls can have unintended and unnecessary consequences on good customers — and their income statements.

Survey results suggest that mobile RDC losses — even if under-reported given the challenges noted above — appear to be at parity with other channels.

Celent analyst Bob Meara, stated, "With the growth of mRDC popularity, it is incumbent upon banks to both be vigilant and to use the best tools available to manage what will certainly be increasing risks associated with RDC."

Recommendations

Mobile Deposit Basics and low hanging fruit

1. **Smart Limits –** based on attributes such as account tenure, risk score or account type
2. **Endorsement Analytics** – Endorsement detection, restrictive endorsement policy and utilization of the restrictive endorsement feature in mobile deposit
3. **Policy Rules** – Flag leading indicators of account abuse (e.g. cash in and out velocity) or blocking money order deposits. Or f*unds availability to account or transaction profile*
4. **Duplicate Deposit Checking** – Implement cross-channel, cross-bank visibility for duplicate deposit detection. These services also return flags when additional risk indicators are present.
5. **Mobile Authentication** – Authenticate the customer, device and account at the carrier level, monitor for changes in the device/account owner information, validate if person is authorized on behalf of the mobile account.
6. **Business Intelligence –** Ensure that the necessary tracking, measurement and reporting processes are in place. Minimally, these should include the amount and type of losses by channel and false positive rates.
7. **Predictive analytics or "scores**" – in mobile RDC might predict the probability of account abuse, duplicate deposit or other forms of fraud.
8. **Test and Learn (Experimental Design) –** Test tailored limits and funds availability modifications with a random sample of customers or with a specific segment where a hypothesis can be tested and then track impact on key portfolio indicators.

To learn more visit www.remotedepositcapture.com and watch the webinar series on this topic.