PaymentsFirst
Service · Education · Support

Member Quick Reference

RDC

RISK MITIGATION & SOUND BUSINESS PRACTICES

- Involve all stakeholders — BSA, Compliance, IT, IS, Business Continuity, Internal Audit, Accounting, Legal
- Identify delivery channels
- Document board approved policies for each delivery channel
- Document procedures for all delivery channels, inclusive of risk-based approval, review processes, setup, training, monitoring
- Initial risk assessment with annual updates; ensure RDC is compatible with business strategies and ability to manage inherent risk
- Monitor for suspicious activities—cross channel, in-channel, behavior, source, money laundering, IP address and geographic monitoring
- Implement multifactor authentication, layered security, anomaly detection, etc.
- For business accounts, layered security should include: enhanced controls for system administrators granted privileges to set up or change system configurations, such as setting access privileges, and application configurations and/or limitation
- Enhanced account activity controls, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)
- Control over changes to account maintenance activities performed by customers either online or through customer service channels
- Well-constructed agreements with responsibilities of each party defined including secure storage and destruction, indorsement standards, duplicate items, deposit, equipment and maintenance, timeframes, limits, mandated controls, fees, etc.
- Require restrictive indorsement for all delivery channels
- Set deposit limits based on customer and delivery channel
- Employee training and customer awareness/training
- If no activity, remove access
- Board reporting and strategic planning
- Business continuity plan with recovery strategies and interim processes if system is not available
- Implement fraud detection and monitoring systems that include consideration of customer history and behavior, and enable a timely and effective response from the financial institution
- Implement on-site visits and annual reviews when warranted based on perceived risk
- Document vendor management program
- Mobile RDC — prequalifying customers, length of time as a customer, other products used, chargebacks, deposit history, average balance, incidents, overdrafts, credit score, pictures of front and back, restrictive indorsement, limits, etc.

Information provided is not inclusive of all sound business practices related to remote deposit capture controls; financial institutions must adapt controls to their own internal environment.

Delivery Channels

- Merchant/Corporate Capture
- Mobile Capture – Corporate/Small Business
- Mobile Capture – Consumer
- Branch Capture, Teller Capture, ATM Capture, Lockbox Capture
- Correspondent Remote Deposit Capture – Foreign and/or Domestic

To Mitigate Risk, FI Must Know:

- Delivery channels
- Number of customers
- Determine deposit limits—consumer, small business, corporate — daily, monthly
- Define funds availability
- Vendor and software – could be different based on channel
- How many scanners in the field, at the branch, per teller
- Types of scanners used
- ATM capture system
- Scanners at correspondent locations
- Scanners in foreign locations

Customer Due Diligence

- Existing customers — CIP in BSA
- For new customers:
  - Business type, geographic location, customer base, third-party relationships

RDC System Controls

- Image Quality Analysis
- Deposit Value and Volume Limits
- CAR/LAR
- Duplicate, Indorsement Detection
- Device ID
- Delay Availability
- Check Verification/Guaranty
- Balance Detection
- Cross-Channel Duplicate Detection

PaymentsFirst Member Support
866-993-3753 info@paymentsfirst.org
678-384-9791 www.paymentsfirst.org

PaymentsFirst
Service · Education · Support