



# ACING YOUR REMOTE DEPOSIT CAPTURE AUDIT: LESSONS FROM BANKERS WHO HAVE “BEEN THERE AND DONE THAT!”



## COMPLIANCE STARTS AT THE TOP

Many banks are becoming savvy about how to “ace their audits” after experiencing more than one FFIEC exam. Below are strategies from two bankers who have, “been there, done that” to help you do just the same.

One of the first steps to streamlining remote deposit capture audits is to develop a policy for the service that your financial institution’s board can review and approve annually, said Brett Miller, a veteran of three remote deposit capture audits. Once the policy is approved, institutions should ensure that their daily remote deposit capture procedures are aligned with the board-approved policy.

Currently, Miller is Assistant Vice President and Product Development Manager for Susquehanna Bancshares. Susquehanna Bancshares is an \$18-billion-asset institution with 245 branches across Maryland, New Jersey, Pennsylvania, and West Virginia. The institution offers diverse product lines, including retail and commercial banking, leasing, wealth management, and capital markets.

Susquehanna Bancshares launched Mobile RDC from Deluxe in March 2013. By early 2014, the financial institution was processing more than 17,000 mobile deposits a month on behalf of over 20,000 enrolled users. In April 2013, Susquehanna Bancshares began converting its Merchant RDC customers from the existing solution to Deluxe’s RDC product. Currently, the institution is processing more than 200,000 transactions per month from over 800 merchants.



REMOTE CAPTURE

“If you say your bank is doing something, make sure the bank is doing it.”

Brett Miller,  
Assistant Vice President  
and  
Product Development  
Manager, Susquehanna  
Bancshares

Miller’s first RDC audit was with First National Bank of Chester County (FNBCC) in 2009. FNBCC was a \$1.1-billion-asset financial institution with 25 banking offices that was acquired by Tower Bancorp. About 100 merchants used FNBCC’s RDC service.

**During FNBCC’s remote deposit capture audit, Miller learned several valuable lessons:**

- The importance of a formal RDC risk assessment program
- The importance of formal RDC policies and procedures
- The need to include customer responsibilities, including the customer’s role in security and document retention requirements, in the institution’s remote deposit capture agreement
- The need to include remote deposit capture in the institution’s business continuity plan

“When the bank initially rolled-out remote deposit capture, we didn’t have documented procedures or a board-approved policy for the service, our customer agreement was only about two pages, and remote deposit capture was not part of the bank’s business continuity plan,” Miller explained.

In addition to addressing these issues, FNBCC also implemented deposit limits for monitoring merchant deposits and an annual review process for remote deposit capture customers.

Miller’s second remote deposit capture audit was with Tower Bancorp in 2011. Tower Bancorp was a \$2.7-billion-asset financial institution that was acquired by Susquehanna Bancshares in 2012. About 300 merchants used Tower Bancorp’s remote deposit capture service at the time of the audit.



REMOTE CAPTURE

“The federal reserve examiners wanted to know how the bank ensures that the responses to our risk assessment form are actually provided by the customer, and are not ‘made up’ by our team. The examiners also wanted to understand whether we train customers on how to transmit deposits, our duplicate detection procedures, and our methodology for establishing risk monitoring business rules.”

Brett Miller,  
Assistant Vice President  
and  
Product Development  
Manager, Susquehanna  
Bancshares

**Miller learned several lessons from the remote deposit capture audit at Tower Bancorp, including:**

- The importance of a strong focus on monitoring customer remote deposit capture activity, specifically, identifying anomalies and/or suspicious patterns in merchant deposits
- The necessity of a comprehensive merchant capture policy with annual board approval
- The importance of updating the financial institution’s remote deposit capture risk assessment plan to encompass a larger market area and customer base as a result of a bank acquisition

“The chief takeaway from the audit was to focus on risk assessment. Tower Bancorp was a small bank that grew quickly and didn’t have a lot of written procedures. The bank completed two acquisitions since its previous remote deposit capture audit was conducted, and, as a result, it was moving into larger metropolitan areas. We were asked to more closely monitor merchant activity, such as large spikes in customer deposit volumes,” Miller said.

In 2013, Susquehanna Bancshares completed both internal and Federal Reserve audits of its remote deposit capture procedures and policies. The bank conducts an internal remote deposit capture audit every 2 years. “Our most recent internal audit focused on procedures for temporary deposit limits and how they integrate with the bank’s credit policy. Our auditors wanted to understand the process for handling over-limit situations,” he said.

**Susquehanna Bancshare’s internal audit also focused on:**

- Scanner inventory: accounting for all of the scanners used by its remote deposit capture customers, and ensuring that the bank is properly billing clients to use the scanners
- System access: ensuring that only employees with relevant job duties can access the system
- Third-party checks: Ensuring that the payee name on the check matches the account name



REMOTE CAPTURE

**Miller said the federal reserve audit largely focused on:**

- **Customer due diligence:** education during customer on-boarding and during the annual customer review, and physical and logical security controls at customer locations
- **Adherence with board-approved policies and procedures:** documenting the daily activities to ensure compliance with the bank's board-approved remote deposit capture policy: "If you say in policy your bank is doing something, make sure the bank is doing it," he said.
- **Duplicate item detection:** enterprise-wide duplicate item detection across all of the bank's remote deposit capture channels (branch, mobile, merchant, automated teller machine)
- **Risk monitoring:** processes and procedures to identify potential deposit risks

"The Federal Reserve examiners wanted know how the bank ensures that the responses to our risk assessment form are accurately outlining the customers control environment" he said. "The examiners also wanted to understand whether we train customers on how to transmit deposits, our duplicate detection procedures, and our methodology for establishing risk monitoring business rules."

Miller said he has learned several valuable lessons from his audits. The first lesson is for financial institutions to diligently document and adhere to procedures for daily remote deposit capture activities, client on-boarding, over-limit approval, credit downgrades, and customer termination. Financial institutions should also develop a customer qualification and due diligence process for initial customer on-boarding and annual account reviews. Finally, he recommended that institutions conduct an annual risk assessment and financially quantify and document all potential risks.



REMOTE CAPTURE

**KNOW YOUR CUSTOMER**

There's no better way to assess the risks of an RDC user than to visit them in-person.

That's according to Beth Gilliard, Senior Vice President, Treasury Management, Texas Citizens Bank. Texas Citizens Bank is a \$380-million-asset financial institution headquartered in Pasadena, Texas, close to Houston. The locally- owned community bank maintains six banking offices local to the Houston area, primarily serving commercial and industrial customers.

“There's no better way to assess the risks of a remote deposit capture user than to visit them in person.”

Beth Gilliard,  
Senior Vice President,  
Treasury Management,  
Texas Citizens Bank

“It takes 45 minutes to travel between our branches,” Gilliard said, adding that few of the bank's remote deposit capture customers are located near a Texas Citizens Bank branch. For this reason, the bank allows business owners to make electronic deposits into their personal accounts. The bank's size creates a unique environment for remote deposit capture in other ways. For instance, temporary over-limit requests are approved by the bank's CEO and chief credit officer, to whom Gilliard reports.

Texas Citizens Bank has used Deluxe's merchant and branch capture solutions for five years. Since 2012, the bank has also used Deluxe's risk monitoring solution. Texas Citizens Bank has over 150 remote deposit capture clients.

Each year, a Texas Citizens Bank employee visits each of the bank's RDC users and completes a 16-question worksheet to assess the customer's adherence to the bank's remote deposit capture policies and procedures, and monitor the customer's financial condition (which may portend issues if the situation is dire). For instance, the worksheet asks bank staff to determine whether the client is promptly deleting the logins of former employees, whether the customer is providing adequate security for the system, how the client is handling check destruction, and how the client's deposit volumes and amounts compare to what the bank originally expected. All of the information collected during the visits is tracked and made available to auditors, Gilliard said.



REMOTE CAPTURE

“Our life would be bad without automated risk monitoring. We can quickly run reports and identify flagged items. Auditors can see what flags are available, and tell us which ones to turn on.”

Beth Gilliard,  
Senior Vice President,  
Treasury Management,  
Texas Citizens Bank

The in-person visits are no small undertaking when you consider that the bank has customers as far away as Dallas and El Paso. It takes the bank a couple of weeks to visit all of its remote deposit capture clients. But Gilliard is convinced the visits help the bank stay ahead of potential issues.

“The annual visits are really about knowing your remote deposit capture customer: how is their business doing overall, and are their procedures according to the Agreement,” Gilliard said, adding that the bank’s lending officer typically visits customers located the furthest away.

Miller noted that Susquehanna Bancshares conducts in-person visits of remote deposit capture users as necessary. But the bank is contemplating site visits to be part of the annual review process.

Texas Citizens Bank began conducting the annual customer visits after the bank completed its first remote deposit capture audit in 2012. During that audit, the bank learned the importance of risk assessment reporting, and daily deposit monitoring and flagging of suspicious transactions.

After its first remote deposit capture audit, Texas Citizens Bank follows a risk assessment matrix that it uses to assess the controls used by customers to mitigate potential risks such as altered or counterfeit items, remotely created checks, changes to a check payee, forged endorsements, altered items, transmission of duplicate images or files, and checks drawn on the company or its affiliates.

**The matrix defines risk levels in three categories:**

1. **HIGH:** potential high-dollar risks that cannot be automatically mitigated by software or other non-discretionary means
2. **MEDIUM:** potential high-dollar risks that can be mitigated by software or other automatic or non-discretionary means
3. **LOW:** low-dollar risks that have been satisfactorily mitigated by wording in the bank’s remote deposit capture agreement, legislation, or regulator interpretation

As a result of the bank’s remote deposit capture audits in 2012, it began logging its annual customer visits, added duplicate item detection across its merchant and branch capture solutions, and placed a greater focus on managing RDC risks with automated risk monitoring.



## REMOTE CAPTURE

Texas Citizens Bank uses Deluxe's risk monitoring solution. The solution automates the identification and tracking of physical capture anomalies and transactions that don't meet established rules for each customer. Rules are applied at the account level for each client. As transactions are captured, each item and deposit is tested based on the established rules for that account. Deposits that exceed limits or violate rules are scored using algorithms that allow bank personnel to review the most suspicious deposits first. Undesirable deposits or items within a deposit can be removed prior to final posting or clearing. Contact information for each account is available in the decisioning interface; making follow up calls or e-mails to the client quick and easy. Comprehensive activity and history reports are available any time to support audit requirements.

"Our life would be difficult without automated risk monitoring," Gilliard said. "We can quickly run reports and identify flagged items. Auditors can see what flags are available, and tell us which ones they consider important." Flagged items are reviewed by the bank's tellers. "They are experienced at looking at checks, so they can quickly identify exceptions. Auditors are sometimes skeptical when you tell them that your Treasury Management staff is reviewing flagged remote deposit capture transactions," Gilliard said.

Every couple of weeks, Gilliard personally reviews flagged items to "see what is happening. It helps with my discussions with auditors." Reviewing electronically deposited items also has enabled Gilliard to spot customers depositing checks drawn from accounts with other banks ("a sign of potential check kiting") as well as customers with loans from nearby banks ("a lending opportunity").

## THE BOTTOM LINE

The FFIEC's guidelines create new risk and audit requirements for financial institutions that offer RDC services to their customers. Financial institutions should not view the guidelines as a reason to delay their RDC initiatives, but more as directional assistance on how to execute. By implementing the lessons learned by bankers who have already completed RDC audits, financial institutions can ace their audits, while mitigating risk and taking full advantage of the technology.



REMOTE CAPTURE

## ARRANGE FOR A PRIVATE CONSULTATION

Deluxe's solutions can help your financial institution ace its FFIEC audit, while taking advantage of the tremendous opportunity in remote deposit capture. The combination of Deluxe's industry expertise and best-in-class RDC solution can help you strengthen existing client relationships, attract new customers, grow deposits, and create a platform for future initiatives.

To arrange for a consultation, call (800) 937-0017 or contact your account representative.



### WANT MORE INFORMATION?

Contact us today.

#### WEB

[fi.deluxe.com](http://fi.deluxe.com)

#### CALL

800.937.0017

...or contact your Deluxe sales representative.

## About Deluxe Financial Services

Deluxe Financial Services is a trusted partner to more than 5,600 financial institutions across North America, including 23 of the top 25 largest treasury management banks. We help our clients succeed in a competitive landscape through a diverse portfolio of best-in-class financial technology solutions. These solutions help clients target, acquire and retain customers; enhance the customer experience; improve efficiency; and optimize commercial and treasury operations.

Industry-leading companies rely on Deluxe Treasury Management Solutions to accelerate working capital, improve straight through processing, better serve their customers, control costs and drive profitable growth with in-house or outsourced offerings for receivables management, remote capture, treasury management onboarding and payment processing services.