

### Remote Deposit Capture Annual Review Checklist

<b>Company Name:</b>	
1) Describe the safeguards used by your organization to ensure the confidentiality & integrity of User Id's and Passwords used to access Remote Deposit Capture	
2) How long do you retain scanned checks before destroying them? ***You are required to destroy scanned checks no earlier than 30 days and no later than 45 days***	
3) Where are your checks stored after being scanned and before being destroyed?	
4) Is your workstation designated for RDC only?	
5) Is your workstation connected directly to the internet or a network router?	
6) Is your workstation protected by a password?	
7) Are any passwords saved on your workstation?	
8) What operating system does your workstation use? - If Windows XP, when do you plan to upgrade?	
9) What operating system service pack does your workstation use? <i>(Go to Start, Programs, Accessories, System Tools, System Information to find out)</i>	
10) Is your workstation physically secured and how?	
11) What type of virus protection/detection program does your organization use on the systems that access Remote Deposit Services?	
12) How often are your virus protection /detection programs updated on the systems that access Remote Deposit Capture?	

<b>13)What is the frequency in which your organization runs a full system virus detection scan on the systems that access Remote Deposit Capture services?</b>	<input type="checkbox"/> Hourly <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Other (Please Specify):
<b>14)Does your organization use a program for malware protection/detection on systems that access Remote Deposit Capture services?</b> <i>(The anti-spyware program can usually be found in the tool bar in the lower right corner of the screen)</i>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>15)If the above answer is Yes (#14): What Malware protection/detection program does your organization use on the systems that access Remote Deposit Capture services?</b>	
<b>16)What is the frequency in which your organization updates its malware protection/detection program?</b> <i>(Right click on the program icon in the tool bar in the lower right corner of the screen to view option and/or statistics)</i>	<input type="checkbox"/> Hourly <input type="checkbox"/> Daily <input type="checkbox"/> Weekly <input type="checkbox"/> Other (Please Specify):
<b>17)What version of Internet Explorer does your organization use to access Remote Deposit Capture?</b>	
<b>18)How frequently are employees trained on information security awareness such as malware, phishing and pharming?</b>	
<b>19)How does your organization keep your Adobe Reader up to date?</b>	
<b>20)Is the line printed on your checks by the scanner clearly legible and does it print on the front or the back of the check?</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Front <input type="checkbox"/> Back
<b>21)Please describe how your organization performs Windows updates and the frequency in which they are performed.</b>	

**COMPANY'S REPRESENTATIVE PERFORMING DEPOSITS:**

Acknowledged By: \_\_\_\_\_ Date: \_\_\_\_\_  
Name and Title

Signature: \_\_\_\_\_

**COMPANY'S INFORMATION TECHNOLOGY REPRESENTATIVE**

Acknowledged By: \_\_\_\_\_ Date: \_\_\_\_\_  
Name and Title

Signature: \_\_\_\_\_

**COMPANY'S AUTHORIZED SIGNER (PER CORPORATE RESOLUTION)**

Acknowledged By: \_\_\_\_\_ Date: \_\_\_\_\_  
Name and Title

Signature: \_\_\_\_\_

**BANK'S REPRESENTATIVE**

Acknowledged By: \_\_\_\_\_ Date: \_\_\_\_\_  
Name and Title

Signature: \_\_\_\_\_

**Email:** [CustomerOperations@fgb.net](mailto:CustomerOperations@fgb.net)

**Fax:** 985-348-0538

**Address:** 400 East Thomas St. Hammond, LA 70401