INWOOD
NATIONAL BANK

Commercial Remote Deposit (Desktop & Mobile) takes the deposit function out of the hands of the bank and places it with the customer. This poses several potential risks such as poor image quality, duplicate items deposited and the security of non-public customer information. Examples of non-public information (NPI) are customer account and routing number, customer address, phone number, date of birth, driver's license number and tax identification number. Many times this information is printed or written on the checks taken by the merchant. It is important that this non-public information be kept secure to mitigate the potential risk of the NPI being compromised and ending up in the hands of unauthorized persons that may use the information in a fraudulent manner.

ACH Origination is a convenient process that introduces customer transactions into the banking system. This poses several potential risks such as duplicate or unauthorized items and the security of non-public customer information. Several examples of non-public information (NPI) are customer account and routing number, and possibly tax identification number. It is important that this non-public information be kept secure to mitigate the potential risk of the NPI being compromised and ending up in the hands of unauthorized persons that may use the information in a fraudulent manner.

Online Wire Transfer places the sending of wires in the hands of our customer. This poses several potential risks such as fraudulent activity, hijacked accounts and loss of account funds. Inwood National Bank has several security procedures to assist you in protecting your funds as well as giving you peace of mind. These measures include call-backs (out-of-band), dual control, behavioral analytics, and repetitive wires to name a few. Several examples of fraud schemes featuring wire payments are business or personal email compromises, commercial account takeover, employee targeting, and vendor invoice fraud.

This survey is a tool for business owners and principals to assist them in identifying, understanding, measuring and mitigating risk. For each question, select the answer that best describes or represents your business practice or environment.

INWOOD
NATIONAL BANK

Computer Security		
1. Does customer have change management program/process in place to: maintain updated and patched operating systems, maintain updated and patched anti-virus software?	Yes	No
2. Do normal users have "Administrator" privileges on their computers?	Yes	No
3. Do you utilize a firewall on your network?	Yes	No
4. Does your network have an Intrusion Detection System (IDS) in place to monitor and protect your network?	Yes	No
5. Is Internet content filtering utilized on your network and computers?	Yes	No
6. Do you utilize wireless technology in your network when using Inwood products & services?	Yes	No
7. Does customer utilize a laptop or mobile device from home and/or travel when using Inwood products & services?	Yes	No
8. Does email pass through a spam filter?	Yes	No
9. If you use applications that require Java and/or Flash, do you keep those programs up-to-date?	Yes	No
10. Do you have a dedicated computer for Inwood products & services?	Yes	No
11. Does customer have designated personnel who administer and monitor user access to Inwood products & services ensuring: only current employees have access, each user has their own user ID, and user IDs are not shared?	Yes	No
12.Does the customer download/retain non-public information from Inwood's products or services?	Yes	No
13. If YES, does the customer protect/secure the downloaded/retained non-public information?	Yes	No
Physical Security		
14. Does customer's facility have appropriate physical security controls (e.g. alarm systems, secure doors, security personnel, etc.)?	Yes	No
Insurance		
15. Does your company have cyber or internet liability insurance coverage?	Yes	No
Emergency Contact		
16. Does customer have instructions of how to inform the bank of any security breaches?	Yes	No

Personnel Security		
17. Are employees required to sign a computer Acceptable Use Policy (AUP)?	Yes	No
18. Does each employee using Inwood products & services receive training regarding computer, Internet, and email security?	Yes	No
19. Do you run background checks on employees prior to hiring?	Yes	No
Remote Deposit Capture Usage		
20. Inspect the scanned items on-hand: Are the items marked in some way when scanned?	Yes	No
21. Inspect the scanning equipment: does scanner appear to produce high quality images?	Yes	No
22. Does customer maintain scanned checks in a secure environment?	Yes	No
23. Does the customer retain scanned checks longer than 30 days?	Yes	No
24. Does the customer destroy scanned checks after retention period days from date of deposit?	Yes	No
Online Wire Usage		
25. Does customer utilize dual control when initiating online wire payments?	Yes	No
26. Does customer have reasonable (non-excessive) online limits set to help limit loss from fraud?	Yes	No
ACH Origination Usage		
27. Does customer utilize dual control when initiating online ACH payments?	Yes	No
28. Does customer have reasonable (non-excessive) online limits set to help limit loss from fraud?	Yes	No
Training		
29. Does customer require/request any training or refresher on proper system usage?	Yes	No

Business Name

Business Description

Completed by

Signature

Account

Date