STONEGATE BANK

Developing an ACH Security Policy

On September 20, 2013, the ACH Security Framework Rule was implemented. The ACH Security Framework establishes minimum data security obligations for ACH Network participants to protect ACH data. The Rule implementation includes three sets of rules, two of which apply to you: (1) Protection of Sensitive Data and Access Controls; and (2) Self-Assessment. As a Stonegate Bank ACH originator, both you and the Bank are required to operate under the NACHA Rules. We have provided this document to assist you in preparing and maintaining a security policy to protect the ACH data used and transmitted by your business.

Protection of Sensitive Data and Access Controls

The ACH Security Framework Rule requires our business customers to establish, implement, and, as appropriate, update security policies, procedures, and systems related to the initiation, processing, and storage of ACH entries. These policies, procedures, and systems must: (a) Protect the confidentiality and integrity of Protected Information; (b) Protect against anticipated threats or hazards to the security or integrity of Protected Information; and (c) Protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

“Protected Information” is the non-public personal information, including financial information, of a person used to create, or contained within, an ACH entry and any related Addenda Record. This not only covers financial information, but also includes sensitive non-financial information (such as health information) that may be incorporated into the Entry or any related Addenda Record. This Rule applies to consumer information only, however, for uniformity we encourage you to apply your procedures and policy so that they cover all customers.

Security policies, procedures, and systems of ACH participants covered by this Rule must include controls on system access that comply with applicable regulatory guidelines. The systems impacted include all systems used by the ACH participant to initiate, process, and store Entries. If your business keeps information about customers in several formats (e.g., on paper, on computers, and online), you should sit down with a team of your employees — an IT person, office manager, etc. — and discuss these issues together to make sure you consider all viewpoints.

- Inventory the types of data you collect, store and/or transmit.
- Inventory how you store your data.
- Inventory where you store your data for each type and format of customer information.
- Inventory how data is moved and who has access.

Take into consideration your type of business and the fixed and portable access devices your employees use to do their jobs. This is a very important part of the inventory process as it will help you begin to identify the potential ways that sensitive data could be inadvertently disclosed. If you think you need outside help to identify potential weaknesses, consider consulting with a data forensics expert.

Inventory the data controls you have in place. Evaluate different types of security procedures and think about whether they make sense for the type of information you maintain, the format in which it is maintained, the likelihood that someone might try to steal the information, and the harm that would result if the information was disclosed. Use the checklists below to assess whether the security measures you are taking are adequate.

1. Inventory the **types of data** you collect, store and/or transmit:

	Yes	No
Name		
Physical Address		
Phone Numbers		
Email Addresses		
Account Numbers		
Invoice Numbers		
Social Security Number		
Driver's License Number		
Business ID Number		
Types and Amounts of Transactions		

2. Inventory **how you store** your data.

	Yes	No
Paper Invoices		
Paper Mailing Lists		
Email Lists		
Paper Customer Files		
Paper Order Requests		
Email		
Databases		
Spreadsheets		
Customer Accounts		
Customer Lists		
Contracts		
Business Plans		
Financial Reports		

3. Inventory **where you store** your data for each type and format of customer information.

PHYSICAL Storage Sites

Physical Storage Site	Yes	No
Desk Drawers		
Filing Cabinets		
Mailroom		
Home Offices		

ELECTRONIC Storage Sites

Device	Yes	No
Desktop Computers		
Laptops		
Servers		
PDAs/Cell Phones/Smart Phones		
USB/Thumb Drives		
CDs/DVDs		
Other Flash Memory Devices		

4. Inventory **how data is moved** and **who has access** to it.

	Connected or Networked?	Who has access?	Does it leave the office?	Is it accessible off-site?	Does it provide internet or email access?
Endpoints					
Desktops					
Laptops					
Servers					
Mobile Devices					
PDAs					
Cell/Smart Phones					
CDs/DVDs					
Flash Memory					

5. Inventory the **data controls you have** (or should have) in place:

Controls / Protection Checklist	Yes	No	If Yes, How?
Computer operating system has all current updates and patches on all machines?			
All endpoint computers have all security devices activated and up-to-date?			
Data Encryption in place — on all machines?			
Electronic data is automatically backed up and can be restored in the event of human error, system failure or natural disaster?			
Sensitive data protected from leaving the business network via outbound email, or portable device (e.g., USB memory stick)?			
Anti-Phishing protections in place?			
Do you and your employees know how to recognize and avoid phishing emails that may enter via business or personal email accounts?			
Malware protections in place against entry via:			
- Business email accounts?			
- The Internet (Web browsers, Web-based email)?			
- Portable storage devices (USB Sticks, iPods) cannot be connected to endpoint machines and download sensitive data without authorization?			

For each item checked "No", develop a plan to implement a solution.

It should be noted that Stonegate Bank has contracted with two vendors, Marble Security™ and IBM® Trusteer Rapport, which assist with protecting against computer viruses, malware incidents, man-in-the-middle, keylogging, phishing, etc. For more information, please visit our website or contact a Commercial Services representative at (877)641-8500.

6. **Write it down**. Record the checklists you've just created, the security measures you are taking, and an explanation of why these security measures make sense. These security measures are the foundation of your security policy.

7. Other items to consider for your policy:

Minimize What You Save & Store

- ✓ Don't keep information you don't absolutely need.
- ✓ Destroy information when it is no longer needed ... and destroy it responsibly.

Use Effective Passwords

- ✓ Never use the default password that may be provided by another company or service provider.
- ✓ Use "strong" passwords that are unique to each user. Strong passwords include some combination of numbers, letters, and symbols. Never use obvious passwords such as your name, your business name, any family member's name, "12345," "ABCDE," "password" or your user name.
- ✓ Change passwords frequently — every 45-60 days.

Block Potential Intruders

- ✓ Restrict computer use to business-only purposes. Malware and viruses can sneak onto business machines when employees use them to visit social networking, personal email and other personal websites.
- ✓ Consider dedicating one computer in your office to online financial use, and do not use that machine for general internet surfing or email.
- ✓ Protect your IT systems from viruses and spyware by using up-to-date antivirus protection and firewalls. Most operating systems and antivirus programs contain an automatic update feature that updates the software as new viruses and spyware become known.
- ✓ Antivirus is not enough. Consider supplementing your antivirus protection and firewalls with other specialized protection tools, such as Intrusion Prevention and anti-spam technologies.
- ✓ Utilize Marble Security and IBM Security Trusteer Rapport, available through Stonegate Bank.

Back-up and Recover Information

- ✓ Reduce business downtime from simple human error, hardware malfunctions or disasters. Put protections in place that will ensure your ready access to data and easy data recovery should any of these occur.
- ✓ Provide for secure off-site storage of your data in case of disaster.

Restrict Access

- ✓ Limit the number of sites/locations where information is stored.
- ✓ Keep paper records in a locked cabinet, or in a room that stays locked when not in use.
- ✓ Limit employees' access to data to only those that need the information to do their job.
- ✓ Separate duties and use available dual control features whenever possible.
- ✓ Take precautions when mailing records. Use a security envelope, require the recipient to sign for the package, and/or ask the delivery service to track the package until it is delivered.
- ✓ Encrypt sensitive electronic information in every online site where it is stored.
- ✓ Many application programs, including Microsoft's Office and Adobe Acrobat, include basic encryption tools for documents you create.
- ✓ If you have a business that electronically stores a great deal of sensitive information, invest in higher-level security software to provide advanced encryption software for desktops, laptops, and removable storage devices.

- ✓ Do not store sensitive information on portable storage devices (e.g., PDA's, USB drives, CD's, laptops, iPhones, iPods, etc.) as these devices are frequently lost or stolen. If this is unavoidable, make sure the information is encrypted.
- ✓ Transmit data over the Internet using only secure connections – often indicated by "https" in the URL bar of your browser. There are several companies that offer relatively inexpensive web-based sites, known as FTP sites, which can transfer data with a secure connection.

In Conclusion - Make a plan using these elements to be certain that the customer data you collect for submission to the ACH network is secure in your office. This assessment and security policy and procedures are not only required by the NACHA Rules, but they also serve to protect your customers, and you, from unnecessary confidential information loss and the potential for financial losses, corporate account takeover, or identity theft.

Your continuance of utilizing Stonegate Bank's ACH origination services obligates you to follow all NACHA Operating Rules, including the ACH Security Framework Rule. If requested, you will provide access to the Bank to review your policies, procedures, and systems to confirm that appropriate care is being taken to protect the impacted consumer information. You may obtain the most current version of the NACHA Rules at www.nacha.org.